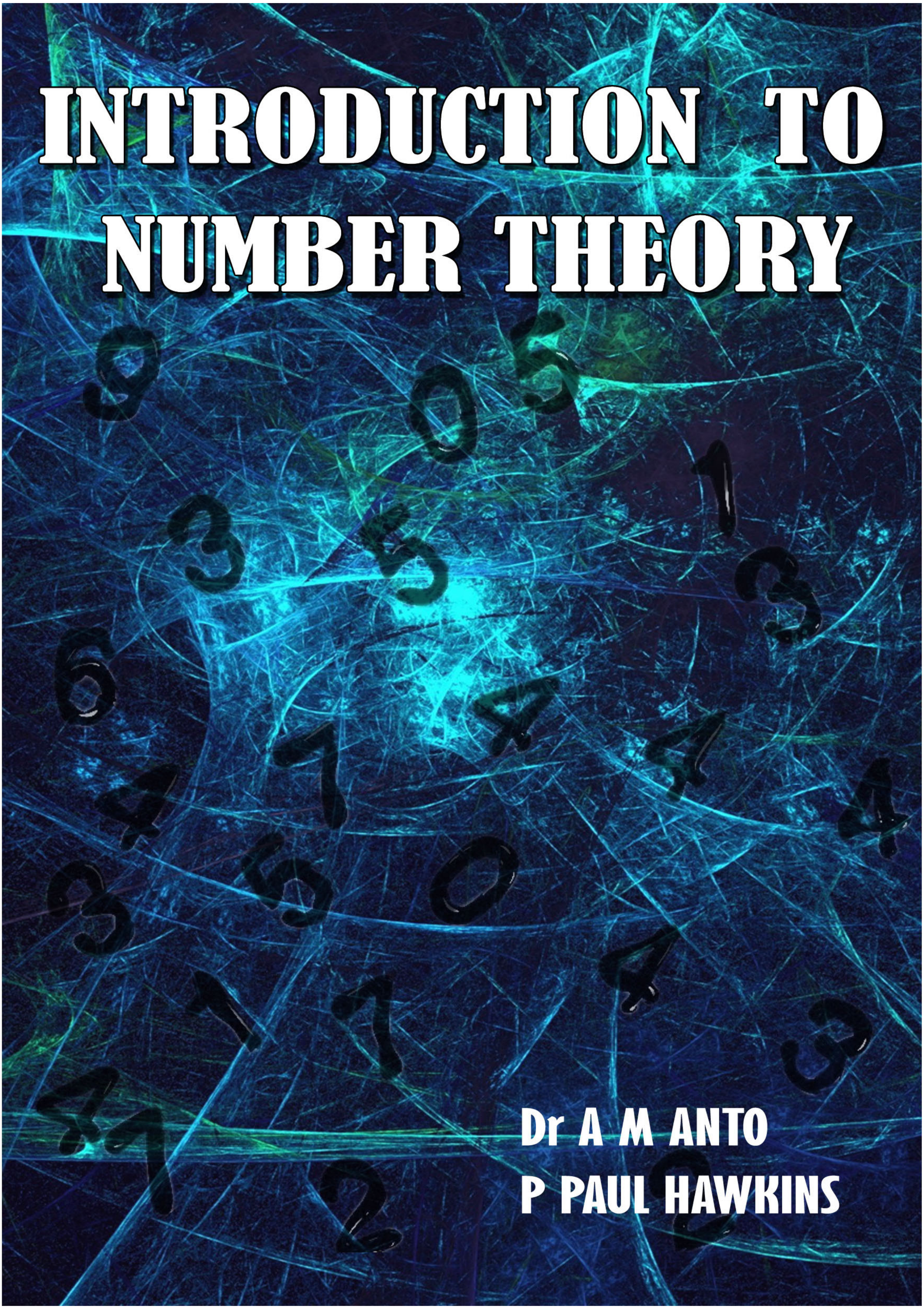
INTRODUCTION TO NUMBER THEORY

INTRODUCTION TO NUMBER THEORY



Dr A M ANTO
P PAUL HAWKINS

INTRODUCTION TO NUMBER THEORY

Dr A.M.ANTO

Assistant Professor
Department of Mathematics
Malankara Catholic College
Kanyakumari 629153

P.PAUL HAWKINS

Assistant Professor
Department of Mathematics
V.T.M College Of Arts and Science
Kanyakumari 629151

Title : Introduction to Number Theory

ISBN : 978-93-88761-28-4

Editors : Dr A.M.ANTO, P.PAUL HAWKINS

Price : 699/-

Published by : **Cape Comorin Publisher**
Kanyakumari, Tamilnadu, India

Printed at :

The Editors and the publisher are not responsible for the statements/opinions expressed by the author(s) of the published articles.

PREFACE

"Introduction to Number Theory" is meant for undergraduate students to help and guide them to understand the basic concepts in Number Theory of five chapters with enumerable solved problems. I am very grateful to thank my department colleagues, students and my friend Dr. R.S. Regin Silvast supported me to finish this book in a successful manner. This book is dedicated to our teacher Dr. E. Ebin Raja Merly. Suggestions and feedback regarding the book is welcomed.

January 2019	Dr A. M ANTO
Kanyakumari	P. PAUL HAWKINS

CONTENT

CHAPTER - I

1.1 The Peano’s Axioms

The axioms of classical arithmetic, which are called Peano’s axioms. It may be written as follows.

(A_1) 0 is a number;

(A_2) The successor of any number is a number;

(A_3) 0 is not the successor of any number;

(A_4) no two numbers have the same successor;

(A_5) If 0 has a property P, and if the successor of a number x has P whenever x has P, then every number has P.

1.2 Mathematical Induction

Well - Ordering principle

Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \leq b$ for all b’s belonging to S.

Theorem 1.1 ***Archimedean property***

If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$

Proof

Given, a and b are any positive integers.

Assume that the statement of the theorem is not true, so that for some a and b, $na < b$ for every positive integer n.

Then the set $S = \left\{\left\{\frac{b-na}{n}\right\}/n \text{ is a positive integer}\right\}$ consists entirely of positive integer. By the well- ordering principle, S will possess a least element, say, $b - ma$.

Also we see that $b - (m + 1)a$ also lies in S, because S contains all integers of this form.

Furthermore, we have $b - (m + 1)a = (b - ma) - a$

$$< b - ma$$

Contrary to the choice of $b - ma$ as the smallest integer in S.

Hence, there exists a positive integer n such that $na \geq b$

Theorem 1.2 ***First principle of finite induction***

Let S be a set of positive integers with the following properties.

a) The integer 1 belongs to S

b) Whenever the integer k is in S, the next integer $k + 1$ must also be in S.

Then S is the set of all positive integers.

Proof

Let S be a set of positive integers.

Let T be the set of all positive integers not in S, and assume that T is nonempty.

Then by the well- ordering principle T possesses a least element, which we denote by a.

Since, $1 \in S$, surely $a > 1$, we have and so $0 < a - 1 < a$.

The choice of a as the smallest positive integer in T implies that $\mathrm{a}-1$ is not a member of T, or $\mathrm{a}-1$ belongs to S.

By hypothesis, S must also contain $(\mathrm{a}-1)+1=\mathrm{a}$, which contradicts the fact that a lies in T therefore we conclude that the set T is empty and in consequence that S contains all the positive integers.

Note

a) $0!=1$

b) $1!=1$

c) $n!=n.(n-1)!$ for $n>1$

PROBLEMS 1.2

Problem 1

Establish the formula below by mathematical induction

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$$

Solution

Let S denote the set of all positive integers n for which

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6} \quad \dots\dots\dots\dots(1)$$

When $n=1$ the formula becomes, $1^2=\frac{1(2)(3)}{6}=1$

This means that $1\in S$

Next we assume that, $k\in S$, So that we have

$$1^2+2^2+\cdots+k^2=\frac{k(k+1)(2k+1)}{6}$$

We prove that, the next integer $k+1$ is also in S

That is $1^2+2^2+\cdots+k^2+(k+1)^2$

$$= \frac{(k+1)(k+1+1)\big(2(k+1+1)\big)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$\mathrm{L.H.S}\ :\ 1^2+2^2+\cdots+k^2+(k+1)^2$

$$= \frac{k(k+1)(2k+1)+6(k+1)^2}{6}$$

$$= \frac{(k+1)}{6}[k(2k+1)+6(k+1)]$$

$$= \frac{(k+1)}{6}[2k^2+7k+6]$$

$$= \frac{(k+1)(2k^2+4k+3k+6)}{6}$$

$$= \frac{(k+1)\big(2k(k+2)+3(k+2)\big)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$$= R.H.S$$

This implies R.H.S is the member of equation (1)

when $n=k+1$.

Therefore, by theorem 1.2, S must be all the positive integers, that is, the given formula is true for $n=1{,}2{,}3\ \ldots\ldots\ldots$..

Problem 2

Establish the formula below by mathematical induction $1^3 + 2^3 + \cdots n^3 = \left[\frac{n(n+1)}{2}\right]^2$ for all $n \geq 1$

Solution

Let S denote the set of all positive integers n for which $1^3 + 2^3 + \cdots n^3 = \left[\frac{n(n+1)}{2}\right]^2$ is true … … … … … (1)

When $n = 1$ the formula becomes, $1^2 = \left[\frac{1(2)^2}{2}\right]^2 = 1$

This means that $1 \in S$

Next we assume that, $k \in S$ so that , we have

$$1^3 + 2^3 + \cdots k^3 = \left[\frac{k(k+1)}{2}\right]^2$$

We prove that, the next integer $(k + 1)$is also in S.

This is, $1^3 + 2^3 + \cdots k^3 + (k+1)^3 = \left[\frac{(k+1)(k+2)}{2}\right]^2$

$L.H.S : 1^3 + 2^3 + \cdots + k^3 + (k+1)^3$

$$= \frac{k^2(k+1)^2}{2^2} + (k+1)^3$$

$$= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}$$

$$= \frac{(k+1)^2}{4} \left(k^2 + 4(k+1)\right)$$

$$= \frac{(k+1)^2}{4} (k^2 + 4k + 4)$$

$$= \frac{(k+1)^2}{4}(k+2)(k+2)$$

$$= \frac{(k+1)^2(k+2)^2}{4}$$

$$= \left[\frac{(k+1)(k+2)}{2}\right]^2$$

$$= R.H.S$$

This implies R.H.S is the member of equation (1) when $n = k + 1$.

Therefore, by theorem 1.2. S must be all the positive integers, that is, the given formulae is true for $n = 1,2,3 \dots \dots$

Problem 3

Establish the formulae below by mathematical induction

$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \geq 1$

Solution

Let S denote the set of all positive integer n for which

$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \geq 1$ is true $\dots \dots \dots .(1)$

When $n = 1$, the formulae becomes, $1 = \frac{1(2)}{2} = 1$

This means that $1 \in S$.

Next we assume that, $k \in S$ so that we have

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

We prove that, the next integers $k + 1$ is also in S.

This is, $1 + 2 + \cdots + k + (k+1) \ = \frac{(k+1)(k+2)}{2}$

$$L.H.S\ :\ 1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$
$$= \frac{k(k+1) + 2(k+1)}{2}$$
$$= \frac{k^2 + 3k + 2}{2}$$
$$= \frac{(k+1)(k+2)}{2}$$
$$= \ R.H.S$$

This implies R.H.S is the member of equation (1) when $n = k + 1$.

Therefore by theorem 1.2 S must be all the positive integers. That is, the given formulae is true for $n = 1{,}2{,}3\ ......$

Problem 4

Establish the formulae below by mathematical induction.

$i)\ 1 + 3 + 5 + \cdots + (2n-1) = n^2\ for\ all\ n \geq 1$

$ii)\ 1.2 + 2.3 + 3.4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$

$for\ all\ n \geq 1$

$iii)\ 1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 \ = \frac{n(2n-1)(2n+1)}{3}$

$for\ all\ n \geq 1$

Solution

$i)$ Let S denote the set of all positive integers n for which

$$1 + 3 + 5 + \cdots + (2n-1) = n^2\ for\ all\ n \geq 1\ is\ true\ ....(1)$$

When $n = 1$ the formula becomes, $(2(1) - 1) = 1 = 1$.

This means that $1 \in S$.

Next we assume that, $k \in S,$ so that we have

$1 + 3 + 5 + \cdots + (2k - 1) = k^2$

We prove that, the next integer $(k + 1)$ is also in S.

That is, $1 + 3 + \cdots + (2k - 1) + (k + 1) = (k + 1)^2$

$$\begin{aligned} L.H.S \ : \ 1 + 3 + \cdots + (2k - 1) + (k + 1) &= k^2 + (k + 1) \\ &= k^2 + k + 1 \\ &= (k + 1)(k + 2) \\ &= (k + 1)^2 \\ &= \ R.H.S \end{aligned}$$

This implies R.H.S is the member of equation (1), when $n = k + 1$

By theorem 1.2 , S must be all the positive integer.

That is, the given formulae is true for $n = 1,2,3\ldots..$

(ii) Let S denote the set of all positive integers a for which

$$1.2 + 2.3 + \cdots + n(n + 1) = \frac{n(n+1)(n+2)}{3} \text{ is true } \ldots\ldots..(1)$$

When $n = 1$ the formulae becomes, $2 = 2 \Rightarrow 1 = 1$.

This means that $1 \in S$.

Next we assume that, $k \in S$.

So that, we have $1.2 + 2.3 + \cdots + k(k + 1) = \frac{k(k+1)(k+2)}{3}$

We prove that, the next integer $(k + 1)$ is also in S.

That is, $1.2 + \cdots + k(k+1) + (k+1)(k+2)$

$$= \frac{(k+1)(k+2)(k+3)}{3}$$

Now, $L.H.S$: $1.2 + \cdots + k(k+1) + (k+1)(k+2)$

$$= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2)$$

$$= \frac{k(k+1)(k+2) + 3\big((k+1) + (k+2)\big)}{3}$$

$$= \frac{(k+1)(k+2)(k+3)}{3}$$

$$= \frac{(k+1)(k+2)(k+3)}{3}$$

$$= R.H.S$$

This implies R.H.S is the member of equation (1) when $n = k + 1$.

Therefore, by theorem 1.2, S must be all the positive integers. That is, the given formulae is true for $n = 1,2,3\ldots\ldots$.

(iii) Let S denote the set of all positive integers n for which

$1^2 + 3^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$ is true .....(1)

When $n = 1$ the formulae becomes,

$$(2-1)^2 = 1 = \frac{1(1)(3)}{3} = 1$$

This means that $1 \in S$.

Next we assume that $k \in S$,

So that we have $1^2 + 3^2 + \cdots + (2k-1)^2 = \frac{k(2k-1)(2k+1)}{3}$

We Prove that, the next integer is $k+1$ is also in S.

That is, $1^2+3^2+\cdots+(2k-1)^2+(k+1)$

$$=\frac{(k+1)(2k+1)(2k+3)}{3}$$

$L.H.S\ :\ 1^2+3^2+\cdots+(2k-1)^2+(k+1)$

$$=\frac{k(2k-1)(2k+1)}{3}+(2k+1)^2$$

$$=\frac{k(2k-1)(2k+1)+3(2k+1)^2}{3}$$

$$=\frac{(2k+1)}{3}\big(k(2k-1)+3(2k+1)\big)$$

$$=\frac{(2k+1)}{3}(2k^2-k+6k+3)$$

$$=\frac{(2k+1)}{3}(2k^2+5k+3)$$

$$=\frac{(2k+1)}{3}(2k+2)(2k+3)$$

$$=\frac{(2k+1)[2k(k+1)+3(k+1)]}{3}$$

$$=\frac{(2k+1)(k+1)(2k+3)}{3}$$

$$=\frac{(k+1)(2k+1)(2k+3)}{3}$$

$$=\ R.H.S$$

This implies R.H.S is the member of equation (1) when $n=k+1$.

Therefore, by theorem 1.2. S Must be the entire positive integer. That is the given formulae is true for $n = 1, 2,3\ldots\ldots$

Problem 5

If $r\neq 1$, show that for any positive integer n,

$$a + ar + ar^2 + \ldots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$

Solution

Let S denote the set of all positive integers n for which $a + ar + ar^2 +, \ldots, +ar^n = \frac{a(r^{n+1}-1)}{r-1}$, $n\geq 1$ and $r\neq 1$ is true ...… (1)

When $n = 1$, $L.H.S = a + ar^1 = a(1 + r)$

$$R.H.S = \frac{a(r^2 - 1)}{r - 1} = a\ (r + 1)$$

Therefore $L.H.S = R.H.S$

This means that $1 \in S$.

Next we assume that, $k \in S$, so that

$$a + ar + a^2 + ar^2 + \cdots + ar^k = \frac{a(r^{k+1} - 1)}{r - 1}$$

We prove that the next integer $k + 1$ is also is S

That is $a + ar + a^2 + ar^2 +, \ldots, +ar^k$

$$= \frac{a(r^{k+1} - 1)}{r - 1} + ar^{k+1}$$

$$= \frac{a(r^{k+1} - 1)}{r - 1} + \frac{ar^{k+1}(r - 1)}{r - 1}$$

$$= \frac{ar^{k+1} - a + ar^{k+2} - ar^{k+1}}{r-1}$$

$$= \frac{ar^{k+2} - a}{r-1}$$

$$= \frac{a(r^{k+2} - 1)}{r-1}$$

Hence $a + ar + a^2 + ar^2 + \cdots + ar^k + \ ar^{k+1} = \frac{a\left(r^{k+2} - 1\right)}{r-1}$

Therefore $k + 1 \in S$

That is equation (1) is true when $n = k + 1$

By theorem 1.2 S must be all the positive integer. That is the given formula is true for $n = 1,2,3$ … … … ..

Problem 6

Prove that the cube of any integer can be written as the difference of two Squares.

$$\left[\begin{aligned} \text{Hint: Notice that } n^3 &= (1^3 + 2^3 + \cdots + n^3) \\ &= \left[\frac{n(n+1)}{2}\right]^2, n \geq 1 \end{aligned}\right]$$

Solution

We have $n^3 = \left[\frac{n(n+1)}{2}\right]^2 - \left[\frac{(n-1)n}{2}\right]^2$

Case $(\boldsymbol{i})$ n is an odd number.

Then $n - 1$ and $n + 1$ are even number, so $\frac{n+1}{2}$ and $\frac{n-1}{2}$ are integers.

Case $(\boldsymbol{ii})$ n is an even number.

Then $\frac{n}{2}$ is an integer

Therefore n^3 is the difference of two Squares

Problem 7

a) Find the value of $n \leq 7$ for which $n! + 1$ is a perfect square

(It is unknown whether $n! + 1$ is a square for any $n > 7$)

b) True or false? For positive integers m and n, $(mn)! = m!\,n!$ and $(m + n)! = m! + n!$

Solution

a) For $n = 1$ then $n! + 1 = 2$ is not a perfect square

For $n = 2$ then $n! + 1 = 3$ is not a perfect square

For $n = 3$ then $n! + 1 = 7$ is not a perfect square

For $n = 4$ then $n! + 1 = 25 = 5^2$ is a perfect square

For $n = 5$ then $n! + 1 = 121 = 11^2$ is a perfect square

For $n = 6$ then $n! + 1 = 721$ is not a perfect square

For $n = 7$ then $n! + 1 = 5041 = 71^2$ is a perfect square

b) False

For example $(3\ 2)! = 720 \neq 3!\,.2! = 6.2 = 12$

$(2 + 3)! = 120 \neq 2! + 3! = 2 + 6 = 8$

Problem 8

Use mathematical induction to derive the formula for all $n \geq 1$:

$1(1!) + 2(2!) + 3(3!) + \cdots + n(n + 1)! - 1$

Solution

Let S denote the set of all positive integer n for which $1(1!) + 2(2!) + 3(3!) + \cdots + n(n+1)! - 1$ is true $\dots\dots..(1)$

When $n = 1$ the formula becomes $1(1+1)! - 1 = 2 - 1 = 1$

This means that $1 \in S$

Next we assume that, $k \in S$ so that,

$1(1!) + 2(2!) + \cdots + k(k+1) = (k+1)! - 1$

We prove that the next integer $k + 1$ is also in S

That is $1(1!) + 2(2!) + \cdots + k(k+1) + (k+1)!$

$$= (k+2)! - 1$$

Now, L.H.S $= 1(1!) + \cdots + k(k!) + (K+1)!$

$$= [(k+1)! - 1] + (k+1)[(k+1)!]$$

$$= (k+1)!\left[1 - \frac{1}{(k+1)!} + (k+1)\right]$$

$$= (k+1)!\left[1 - \frac{1}{(k+1)!} + k + 1\right]$$

$$= (k+1)!\left[(k+2) - \frac{1}{(k+1)!}\right]$$

$$= (k+1)!\,(k+2) - \frac{(k+1)!}{(k+1)!}$$

$$= (k+2)! - 1$$

$$= R.H.S$$

This implies $R.H.S$ is the member of equation (1) when $n = k + 1$

Therefore, by theorem 1.2 S must be the entire positive integer.

That is, the given formula is true for $n = 1,2,3 \dots \dots ....$

Problem 9

a) Verify that for all $n \geq 1$ **,** $2.6.10.14 \dots .. (4n-2) = \frac{(2n)!}{n!}$

b) Use part (a) to obtain the inequality $2^n (n!)^2 \leq (2n)!$

for all $n \geq 1$

Solution

(a) Let S denote the set of all positive integers for which

$2.6.10.14 \dots .. (4n-2) = \frac{(2n)!}{n!}$ is true $\dots \dots \dots .. (1)$

When $n = 1$ the formula becomes $2 = 2 \implies 1 = 1$

This means that $1 \in S$

Next we assume that, $k \in S$ so that

$$2.6.10.14 \dots .. (4k-2) = \frac{(2k)!}{k!}$$

We prove that the next integer $k+1$ is also is S, that is,

$2.6.10. \dots .. (4k-2)(4k+2) = \frac{(2k+2)!}{(k+1)!}$ is true

$$L.H.S:\ 2.6.10.14 \dots .. (4k-2)(4k+2) = \frac{(2k)!}{k!}(4k+2)$$

$$= \frac{(2k1)!}{k!} 2(2k+1)$$

$$= \frac{2k(2k-1)!}{k!}\ 2(2k+1)$$

$$=\frac{2k(2k+1)!}{k!}\,\frac{2k+2}{2k+2}\frac{2(2k+2)!}{2k!\,(k+1)}$$

$$=\frac{(2k+2)!}{(k+1)!}$$

$$=R.H.S$$

This implies R.H.S is the member of equation (1) when $n=k+1$

By theorem $(1.2), S$ must be the entire five integers.

That is the given formula is true for $n=1,2,\ldots..$

b) From (a), we have $(2n)!=2.6.10\ldots(4n-2)(n!)$

So the problem is reduces to $2^n(n!)^2\leq 2.6.10\ldots(4n-2)(n!)$

Which implies $2^n(n!)\leq 2.6.10\ldots(4n-2)$

Let S denote the set of all positive integer n for which $2^n(n!)\leq 2.6.10\ldots(4n-2)$ is true $\ldots\ldots\ldots..(1)$

When $n=1$ the formula becomes $2^1(1!)(1!)=2\leq 2$

This means that $1\in S$

Next we assume that $k\in S$ so that $2^k(k!)\leq 2.6.10\ldots(4k-2)$

We prove that the next integer $k+1$ is also in S

That implies $2^{k+1}(k+1!)\leq 2.6.10\ldots(4(k+1)-2)$

Now, L.H.S $=2^{k+1}(k+1!)$

$$=2^k(k!)2.(k+1)$$

$$=2^k(k!)(2k+2)$$

$$\leq 2^k(k!)(4k+2)$$

$$\leq 2.6.10\ldots(4k-2)(4k+2)$$

$$= 2.6.10 \ldots (4(k+1)-2)$$

$$= \text{R.H.S}$$

Therefore, $L.H.S \leq R.H.S$

By theorem $1.2.S$ must be the entire positive integer that is the given formula, is true for $n = 1,2,3....$

Problem 10

Establish the Bernoulli inequality if $1 + a > 0$

then $(1+a)^n \geq 1 + na$ for all $n \geq 1$

Solution

Let S denote the set of all positive integer n for which $(1+a)^n \geq 1 + na, n \geq 1$ is true $\ldots\ldots\ldots\ldots.(1)$

When $n = 1,$ the formula becomes $(1+a) \geq 1 + a$, this means that $1 \in S$

Next we assume that $k \in S$ so that the equation $(1+a)^k \geq 1 + ka \ldots\ldots..(2)$

We prove that the next integer $k+1$ is also in S, that is, to prove $(1+a)^{k+1} \geq 1 + (k+1)a$

$$\text{L.H.S} = (1+a)^{k+1}$$

$$= (1+a)^k.(1+a)$$

$$\geq (1+ka).(1+a)$$

$$= 1 + ka + a + ka^2$$

$$\geq 1 + ka + a \;(Since\; a^2 > 0, So\; ka^2 > 0)$$

$$= 1 + (k+1)a$$

$= R.H.S$

Therefore $L.H.S \geq R.H.S$

This implies (1) is true when $n = k + 1$

By theorem 1.2. S must be all positive integer

That is, the given formula is true for $n = 1,2,3$ ....

Problem 11

Consider the Lucas sequence $1,3,4,7,11,18,29,47,76$ .... prove that $a_n < \left(\frac{7}{4}\right)^n$ for all $n \geq 1$

Solution

Except for the first two terms of each terms of the sequence is the sum of the preceding two, so that the sequence may be defined inductively by $a_1 = 1, a_2 = 3 \; and \; a_n = a_{n-1} + \; a_{n-2}$ for all $n \geq 1$

We prove that, $a_n < \left(\frac{7}{4}\right)^n$ for every positive integer n

When $n = 1, a_1 = 1 < \left(\frac{7}{4}\right)^1$ therefore, the result is true when $n = 1$

When $n = 2, a_2 = 3 < \left(\frac{7}{4}\right)^2 = \left(\frac{49}{16}\right)$

$\Rightarrow \quad 3 < 3.0625$

Therefore, the result is true when $n = 2$

For the induction step choose an integer $k \geq 3$ and assume that the inequality is valid for $n = 1,2, \ldots k - 1$

That is we have, $a_{k-1} < \left({}^{7}/_{4}\right)^{k-2}$

Then prove that the result is true for k.

Now, $a_k = a_{k-1} + a_{k-2}$

$$< \left({}^{7}/_{4}\right)^{k-1} + \left({}^{7}/_{4}\right)^{k-2}$$

$$= \left({}^{7}/_{4}\right)^{k-2} \left(\left({}^{7}/_{4}\right) + 1\right)$$

$$= \left({}^{7}/_{4}\right)^{k-2} \left(\frac{11}{4}\right)$$

$$= \left({}^{7}/_{4}\right)^{k-2} . \left({}^{7}/_{4}\right)^{2}$$

$$< \left({}^{7}/_{4}\right)^{k}$$

Therefore, $a_k < \left({}^{7}/_{4}\right)^{k}$

Because the inequality is true for $n = k$, whenever it is true for the integers $1,2,3, \dots . k - 1$.We conclude by the second induction principle that $a_n < \left({}^{7}/_{4}\right)^{n}$For all $n \geq 1$

Problem 12

Suppose that the numbers a_n are define inductively by $a_1 = 1, a_2 = 2,\ a_3 = 3$ and $a_n = a_{n-2} + a_{n-3}\ for\ all\ n \geq 4.$ Use the second Principle of Finite Induction to show that $a_n < 2^n$ for every positive integer n.

Solution

We have to prove that, $a_n < 2^n$ for every positive integer n

When $n = 1, a_1 \ < 2$, that is, $1 < 2$

Therefore, the result is true when $n = 1$

When $n = 2$, $a_2 < 4$

That is, $2 < 4$

Therefore, the result is true when $n = 2$

When $n = 3, a_3 < 8$

That is, $3 > 8$

Therefore, the result is true when $n = 3$

For the induction step choose an integer $k \geq 4$ and assure that the inequality is valid for $n = 1,2, \dots, k - 1$.

Then, in particular, we have $a_{k-1} < 2^{k-1}$, $a_{k-2} < 2^{k-2}$ and $a_{k-3} < 2^{k-3}$

To prove that the result is true for k

Now, $\quad a_k = a_{k-1} + a_{k-2} + a_{k-3}$

$$\begin{aligned} &\leq 2^{k-1} + 2^{k-2} + a^{k-3} \\ &= 2^{k-3}\,(2^2 + 2 + 1) \\ &= 2^{k-3}(7) \\ &< 2^{k-3}\,.\,2^3 \\ &< 2^k \end{aligned}$$

Therefore, we have $a_k \ < 2_k$

Because the inequality is true for $n = k$ whenever it is true for the integers $1,2, \dots \dots k - 1$

We conclude by the second induction principle that $a_n < 2^n$ for all $n \neq 4$

Problem 13

If the numbers a_n are defined by $a_1 = 11\,, a_2 = 21$ and $a_n = 3a_{n-1} - 2a_{n-2}\, for$ all $n \geq 3$, prove that $a_n = 5.\,2^n + 1$ for all $n \geq 1$ by second principle of finite induction.

Solution

Given, $a_1 = 11, a_2 = 21, a_n = 3a_{n-1} - 2a_{n-2}$ for all $n \geq 3$

We prove that $a_n = 5.\,2^n + 1$ for all $n \geq 1$

When $n = 1, a_1 = 10 + 1 \Longrightarrow a_1 = 11$

Therefore, the result is true when $n = 1$

When $n = 2,\;\; a_2 = 5.4 + 1 = 21$

Therefore, $a_2 = 21$

Hence, the result is true when $n = 2,$

For the induction step choose an integer $k \geq 3$ and assume that the inequality is valid for $n = 1,2, \dots \dots k - 1$

Then in particular we have $a_{k-2} = 5.2^{k-2} + 1$ and $a_{k-1} = 5.2^{k-1} + 1$

To prove the result is true for k

Now, $a_k = 3a_{k-1} - 2a_{k-2}$

$$= 3(5.2^{k-1} + 1) - 2(5.2^{k-1} + 1)$$

$$= 15.2^{k-1} + 3 - 10.\,2^{k-2} - 2$$

$$= 15.2^{k-1} - 10.\,2^{k-2} + 1$$

$$= 2^{k-2}(15.2 - 10) + 1$$

$$= 2^{k-2}(20) + 1$$

$$= 2^{k-2}5.2^2 + 1$$

$$= 2^{k-2+2}.5 + 1$$

Therefore, $a_k = 5.2^k + 1$

Because the inequality is true for $n = k$ whenever it is true for the integer $1,2, \dots \dots k - 1.$

We conclude by the second induction principle that $a_n = 5.2^n$ for all $n \geq 1$

Exercise

1. Prove that $n! > n^2$ for every integer $n \geq 4,$ whereas $n! > n^3$ for every integer $n \geq 6$
2. For all $n \geq 1,$ prove the following by Mathematical Induction

   $a)\ \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$

   $b)\ \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{n1}{2^n} = 2 - \frac{n+2}{2^n}$
3. Show that the expression $\frac{(2n)!}{2^n.n!}$ is an integer for all $n \geq 0$
4. Use the second principle of Finite induction to establish that for all $n \geq 1$

   $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + \cdots + a + 1)$

   [Hint: $a^{n+1} - 1 = (a+1)(a^n - 1) - a(a^{n-1} -$ 1-1)]

1.3 The Binomial Theorem:

Binomial coefficients

The term binomial coefficient was introduced by the German algebraist Michel Stifle $(1486 - 1567)$. In his best known work, Arithmetica Integra (1544),Stifle gives the binomial coefficients for $n \leq 17$.

Definition

Let n and r be non-negative integers. The binomial coefficient $\binom{n}{r}$ is defined by $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ if $r \leq n,$ and is 0 otherwise, it is also denoted by $c(n, r)$ and nC_r.

For example,

$$\binom{5}{3} = \frac{5!}{3!\,(5-3)!} = \frac{5.4.3.2.1}{3.2.1.2.1} = 10$$

Note

$i)$ $\binom{n}{0} = 1 = \binom{n}{n}$

$ii)$ There are many instances when we need to compute the binomial coefficients $\binom{n}{r}$ and $\binom{n}{n-r}$.

Since $\binom{n}{n-r} = \frac{n!}{(n-r)[n-(n-r)]!}$

$$= \frac{n!}{(n-r)!\,r!}$$

$$= \frac{n!}{r!\,(n-r)!}$$

$$=\binom{n}{r}$$

For example, $\binom{25}{20}=\binom{25}{25-20}=\binom{25}{5}=53{,}130.$

The following theorem shows an important recurrence relation satisfied by binomial coefficients. It is called Pascal's identity, after the outstanding French mathematician and philosopher Blaise Pascal.

Theorem 1.3 ***Pascal's Rule***

Let n and r be positive integers, where $r \leq n$.

Then $\binom{n}{r}=\binom{n-1}{r-1}+\binom{n-1}{r}$

Proof

We shall simplify the R.H.S and show that it is equal to the L.H.S

$$\binom{n-1}{r-1}+\binom{n-1}{r}=\frac{(n-1)!}{(r-1)(n-r)!}+\frac{(n-1)!}{r!\,(n-r-1)!}$$

$$=\frac{r(n-1)!}{(r-1)!\,r(n-r)!}+\frac{(n-r)(n-1)!}{r!\,(n-r-1)!\,(n-r)}$$

$$=\frac{r(n-1)!}{r!\,(n-r)!}+\frac{(n-r)(n-1)!}{r!\,(n-r)!}$$

$$=\frac{(n-1)!\,[r+(n-r)]}{r!\,(n-r)!}$$

$$=\frac{(n-1)!\,n}{r!\,(n-r)!}=\frac{n!}{r!\,(n-r)!}=\binom{n}{r}$$

Theorem 1.4 ***The Binomial Theorem***

The general binomial expansion takes the form,

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1} + \binom{n}{2}a^{n-2}b^2$$

$$+\cdots..+\binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

$$ie, (a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

Proof

We prove the binomial expansion by mathematical induction.

When $n = 1$ the formulae is reduces to

$$(a+b)^1 = \sum_{k=0}^{1}\binom{1}{k}a^{1-k}\,b^k = \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1$$

$$= a + b$$

Therefore, the formula is true when $n = 1$

Assuming that the formula holds for some fixed integer m.

That is, $(a+b)^m = \sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k \dots\dots\dots..(1)$

We prove that it also must holds for $m+1$.

We have to notice that, $(a+b)^{m+1} = (a+b)^m(a+b)$

$$= a(a+b)^m + b(a+b)^m$$

But under the induction hypothesis,

$$a(a+b)^m = \sum_{k=0}^{m}\binom{m}{k}a^{m-k+1}b^k \qquad \text{by } (1)$$

$$= a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m+1-k} b^k$$

and $b(a+b)^m = \sum_{j=0}^{m} \binom{m}{j} a^{m-j}\, b^{j+1}$ by (1)

$$= \sum_{k=1}^{m+1} \binom{m}{k-1} a^{m+1-k} b^k$$

$$= \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k} b^k + b^{m+1}$$

Therefore,

$$a(a+b)^m + b(a+b)^m = a^{m+1} + \sum_{k+1}^{m} \binom{m}{k} a^{m+1-k} b^k$$

$$+ \sum_{k=1}^{m} \binom{m}{k-1} a^{m+1-k}\, b^k + b^{m+1}$$

$$= a^{m+1} + \sum_{k=1}^{m} \left[\binom{m}{k} + \binom{m}{k-1}\right] a^{m+1-k} b^k + b^{m+1}$$

$= a^{m+1} \sum_{k=1}^{m} \binom{m+1}{k} a^{m+1-k} + b^{m+1}$ by Pascal's rule

Therefore, $(a+b)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k}. b^k$

Hence, the formula is true when $n = m + 1$

This establishes the binomial theorem by induction.

PROBLEMS 1.3

Problem 1

a) Derive Newton’s identity

$$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}\ , \ \ n \geq k \geq r \geq 0$$

b) Use part (a) to express $\binom{n}{k}$ in terms of its predecessor

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}, n \geq k \geq 1$$

Solution

a) L.H.S $= \binom{n}{k}\binom{k}{r}\ \ ,\ \ n \geq k \geq r \geq 0$

Therefore, $\dfrac{n!}{k!\,(n-k)!}\cdot\dfrac{k!}{r!\,(k-r)!} = \dfrac{n!}{r!}\cdot\dfrac{1}{(n-k)!\,(k-r)!}$

$$= \frac{n!}{r!}\cdot\frac{(n-r)!}{(n-r)!}\cdot\frac{1}{(n-k)!\,(k-r)!}$$

$$= \frac{n!}{r!\,(n-r)!}\cdot\frac{(n-r)!}{(k-r)!\,(n-k)!}$$

$$= \binom{n}{r}\cdot\frac{(n-r)!}{(k-r)!\,[n-r-(k-r)]!}$$

$$= \binom{n}{r}\cdot\binom{n-r}{k-r}$$

b) To use part (a), Put $r = 1$

Then, $\binom{n}{k}\binom{k}{1} = \binom{n}{1}\binom{n-1}{k-1}\ \ ,\ \ n \geq k \geq r \geq 0$

So, $\binom{n}{k}k = n\binom{n-1}{k-1}$

$$= n\frac{(n-1)!}{(k-1)!\,(n-k)!}$$

$$= \frac{n!}{(k-1)!\,(n-k+1)!}.(n-k+1)$$

So, $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$

Problem 2

If $2 \le k \le n-2$, Show that $\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$ $, n \ge 4$

Solution

Given that $2 \le k \le n-2 \; and \; n \ge 4$

$$\text{L.H.S} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}$$

$$= \frac{(n-2)!}{(k-2)!\,(n-k)!} + \frac{2(n-2)!}{(k-1)!\,(n-k-1)!} + \frac{(n-2)!}{k!\,(n-k-2)!}$$

$$= \frac{k(k-1)!\,(n-2)!}{k!\,(n-k)!} + \frac{2k(n-k)(n-2)!}{k!\,(n-k)!}$$

$$+ \frac{(n-k)!\,(n-k-1)!\,(n-2)!}{k!\,(n-k)!}$$

$$= \frac{(n-2)!\,[k^2 - k + 2kn - 2k^2 + n^2 - nk - n - kn + k^2 + k]}{k!\,(n-k)!}$$

$$= \frac{(n-2)!\,[n^2 - n]}{k!\,(n-k)!}$$

$$= \frac{n(n-1)(n-2)!}{k!\,(n-k)!} = \binom{n}{k}$$

Since $2 \leq k$, for the expansion of $(k-2)!$ the denominator $n-k-2 \geq 0$ or $n-2 \geq k \geq 2$, so $n \geq 4$ for $(n-k-2)!$ in denominator to work.

Problem 3

For $n \geq 1$, derive each of the identities below

a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$

[Hint: Let $a = b = 1$ in binomial theorem]

b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^n\binom{n}{n} = 0$

c) $\binom{n}{0} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1}$

[Hint : After expanding $n(1+b)^{n-1}$ by the theorem,

let *b=1* note also that *nn−1k=k+1nk+1*

d) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = 3^n$

e) $\binom{n}{0} + \binom{n}{1} + \binom{n}{4} + \binom{n}{6} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}$

[Hint: use parts (a) and (b)]

f) $\binom{n}{0} - \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} \ldots . + \frac{(-1)}{n+1}\binom{n}{n} = \frac{1}{n+1}$

[Hint: The left hand side equals

$$\frac{1}{n+1}\left[\binom{n+1}{1} - \binom{n+1}{2} + \binom{n+1}{3} \ldots . + (-1)^n\binom{n+1}{n+1}\right]]$$

Solution

a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$

In binomial Theorem, let us take $a = b = 1$, Therefore, $(a+b)^n = 2^n = \sum_{k=0}^{n} 1^{n-k}1^k$

So, $2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$

b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^n \binom{n}{n} = 0$

In binomial Theorem, Let us take $a = 1, b = -1$

Therefore, $0^n = 0 = \binom{n}{0} - \binom{n}{1} + \cdots. +(-1)^n\binom{n}{n}$

c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n} = n2^{n-1}$

In binomial theorem, let us take $a = 1$

Then $(1+b)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} b^k$

So, $n(1+b)^{n-1} = n\left[\binom{n-1}{0} + \binom{n-1}{1} b + \cdots + \binom{n-1}{n-1}^{k-1}\right]$

Now, let take $b = 1,$

Then $n2^{n-1} = n\binom{n-1}{0} + n\binom{n-1}{1} + \cdots + n\binom{n-1}{n-1}$

$$= \sum_{k=0}^{n-1} n\binom{n-1}{k}$$

But $n\binom{n-1}{k} = \frac{n(n-1)!}{k!\,(n-k-1)!} = \frac{n!}{k!\,[n-(k+1)]} . \frac{(k+1}{(k+1)}$

$$= (k+1)\frac{n!}{(k+1)[n-(k+1)]!}$$

$$= (k+1)\binom{n}{k+1}$$

Therefore, $n2^{k-1} = \sum_{k=0}^{n-1} n\binom{n-1}{k} = \sum_{k=0}^{n-1}(k+1)\binom{n}{k+1}$

$$= \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots\ + n\binom{n}{n}$$

d) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots\ + 2^n\binom{n}{n} = 3^n$

In binomial theorem, let us take $a = 1, b = 2$

$$(a+b)^n\ = 3^n\ = \binom{n}{0}1^n + \binom{n}{1}1^{n-1}2 + \cdots\ + \binom{n}{n}2^n$$

$$= \binom{n}{0} + 2\binom{n}{1} + \cdots + 2^n\binom{n}{n}$$

e) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots\ \ = \binom{n}{0} + \binom{n}{3} + \binom{n}{5} + \cdots\ = 2^{n-1}$

Add and subtract results of (a) & (b) If n is even, then last term is positive

$$\left\{\binom{n}{0} + \binom{n}{1} + \cdots\ + \binom{n}{n}\right\} + \left\{\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots\ + \binom{n}{n}\right\}$$

$$= 2^n + 0$$

We get, $2\left\{\binom{n}{0} + \binom{n}{2} \ldots\ + \binom{n}{n}\right\}\ = 2^n$

Therefore, $\binom{n}{0} + \binom{n}{2} \ldots\ + \binom{n}{n} = 2^{n-1}$

If n is odd last term is $-\binom{n}{n}$

$$\left\{\binom{n}{0} + \binom{n}{1} + \cdots\ + \binom{n}{n}\right\} + \left\{\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots - \binom{n}{n}\right\}$$

$$= 2^n + 0$$

$$2\left\{\binom{n}{0} + \binom{n}{2} + \cdots\ + \binom{n}{n-1}\right\}\ = 2^n$$

So, $\binom{n}{0}+\binom{n}{2}+\cdots\binom{n}{n-1}=2^{n-1}$

If n is even, Then last term is positive then,

$$\left\{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}\right\}-\left\{\binom{n}{0}-\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}\right\}$$

$$=2^n-0$$

Therefore,$2\left\{\binom{n}{1}+\binom{n}{3}+\cdots+\binom{n}{n-1}\right\}=2^n$

Hence, $\left\{\binom{n}{1}+\binom{n}{3}+\cdots+\binom{n}{n-1}\right\}=2^{n-1}$

If n is odd, last term is $-\binom{n}{n}$

$$\left\{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}\right\}-\left\{\binom{n}{0}-\binom{n}{1}+\binom{n}{2}+\cdots-\binom{n}{n}\right\}$$

$$=2^n-1$$

Therefore, $2\left\{\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots\binom{n}{n-1}\right\}=2^n$

So, $\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots=2^{n-1}$

f) $\binom{n}{0}-\frac{1}{2}\binom{n}{1}+\frac{1}{3}\binom{n}{2}-\cdots+\frac{(-1)^n}{n+1}\binom{n}{n}=\frac{1}{n+1}$

In this Problem, the k^{th} term can be written as $(-1)^{k-1}.\frac{1}{k}\binom{n}{k-1}$

We note that $\binom{n}{k-1}=\frac{n!}{(k-1)!(n-k+1)!}$

$$=\frac{k}{(n+1)}.\frac{(n+1)!}{k!\,(n-k+1)!}$$

Thus, $\frac{1}{k}\binom{n}{k-1}=\frac{1}{n+1}\binom{n+1}{k}$

So, problem is equivalent to,

$$\binom{n}{0}-\frac{1}{2}\binom{n}{1}+\cdots+\frac{(-1)^n}{n+1}\binom{n}{n}$$

$$=\frac{1}{n+1}\binom{n+1}{1}-\frac{1}{n+1}\binom{n+1}{2}+\cdots+\frac{(-1)^{n+1}}{n+1}\binom{n+1}{n+1}$$

$$=\frac{1}{n+1}\left[\binom{n+1}{1}-\binom{n+1}{2}+\binom{n+1}{3}-\cdots\ (-1)^{n+1}\binom{n+1}{n+1}\right]$$

From (b), we have $\binom{n}{0}=\binom{n}{1}-\binom{n}{2}+\cdots-(-1)^n\binom{n}{n}$

Substituting $n=S+1$

Then we get, $\binom{s+1}{0}=\binom{s+1}{1}-\binom{s+1}{2}+\cdots-(-1)^{s+1}\binom{s+1}{s+1}$

$$ie)\ 1=\binom{s+1}{1}-\binom{s+1}{2}+\cdots+(-1)^{s}\binom{s+1}{s+1}$$

Therefore, $\binom{n}{0}-\frac{1}{2}\binom{n}{1}+\cdots+\frac{(-1)^n}{n+1}\binom{n+1}{(n+1}$

$$=\frac{1}{n+1}\left[\binom{n+1}{1}-\binom{n+1}{2}+\cdots\ (-1)^{n+1}\binom{n+1}{n+1}\right]$$

$$=\frac{1}{n+1}[1]$$

$$=\frac{1}{n+1}$$

Problem 4

Prove the following for $n\geq 1$:

a) $\binom{n}{r}<\binom{n}{r+1}$ if and only if $0\leq r<\frac{1}{2}(n-1)\backslash$

b) $\binom{n}{r}>\binom{n}{r+1}$ if and only if $n-1\geq r>\frac{1}{2}(n-1)$

c) $\binom{n}{r} = \binom{n}{r+1}$ if and only if n is odd integers,

and $r = \frac{1}{2}(n-1)$

Solution

a) For $n \geq 1, \binom{n}{r} < \binom{n}{r+1}$ iff $0 \leq r < \frac{1}{2}(n-1)$

Proof

Now, $\binom{n}{r} < \binom{n}{r+1} \Leftrightarrow \frac{n!}{r!(n-r)!} < \frac{n!}{(r+1)!(n-r-1)!}$,

$$0 \leq r, \;\; 0 \leq n-r-1$$

$$\Leftrightarrow \frac{(r+1)!}{r!} < \frac{(n-r)!}{(n-r-1)!}, \;\; 0 \leq r \leq n-1$$

$$\Leftrightarrow r+1 < n-r, \;\; 0 \leq n-1$$

$$\Leftrightarrow 0 \leq 2r < n-1$$

$$\Leftrightarrow 0 \leq r < r < \frac{1}{2}(n-1)$$

b) $\binom{n}{r} > \binom{n}{r+1}$ if and only if $n-1 \geq r > \frac{1}{2}(n-1)$

Proof

Now, $\binom{n}{r} > \binom{n}{r+1} \Leftrightarrow \frac{n!}{r!(n-r)!} > \frac{n!}{(r+1)!(n-r-1)!}$,

$$r \geq 0, \;\; n-r-1 \geq 0$$

$$\Leftrightarrow \frac{(r+1)!}{r!} > \frac{(n-r)!}{(r+1)!\,(n-r-1)!},$$

$$r \geq 0, \;\; n-r-1 \geq 0$$

$$\Leftrightarrow \frac{(r+1)!}{r!} > \frac{(n-r)!}{(n-r-1)!},$$

$$r \geq 0,\ \ n-r-1 \geq 0$$

$$\Leftrightarrow r+1 > n-r, n-1 \geq r \geq 0$$

$$\Leftrightarrow 2r > n-1, n-1 \geq r \geq 0$$

$$\Leftrightarrow n-1 \geq r > \frac{1}{2}(n-1) \geq 0$$

c) $\binom{n}{r} = \binom{n}{r+1} \Leftrightarrow r = \frac{1}{2}(n-1)$

Proof

We have,

$$\binom{n}{r} = \binom{n}{r+1} \Leftrightarrow \frac{n!}{r!\,(n-r)!} = \frac{n!}{(r+1)!\,(n-r-1)!},$$

$$r \geq 0,\ \ n-r-1 \geq 0$$

$$\Leftrightarrow \frac{(r+1)!}{r!} = \frac{(n-r)!}{(r+1)!\,(n-r-1)!},$$

$$r \geq 0,\ \ n-r-1 \geq 0$$

$$\Leftrightarrow \frac{(r+1)!}{r!} = \frac{(n-r)!}{(n-r-1)!},$$

$$r \geq 0\,,\ \ n-r-1 \geq 0$$

$$\Leftrightarrow r+1 = n-r,\ \ n-1 \geq r \geq 0$$

$$\Leftrightarrow 2r = n-1,\ \ n-1 \geq r \geq 0$$

$$\Leftrightarrow r = \frac{1}{2}(n-1),\ \ n-1 \geq r \geq 0$$

Problem 5

For $n \geq 2$, prove that $\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n}{2} = \binom{n+1}{3}$

Solution

For $n \geq 2, \binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n}{2} = \binom{n+1}{3}$

We prove this by induction on k

For $k = 2, \binom{2}{2} = 1 = \binom{2+1}{3} = 1$

Assume the result is true for k

$ie)$ $\binom{2}{2} + \cdots + \binom{k}{2} = \binom{k+1}{3}$

To prove the result is true for $k + 1$

Let $\binom{2}{2} + \cdots + \binom{k}{2} + \binom{k+1}{2} = \binom{k+1}{3} + \binom{k+1}{2}$

$= \binom{k+1}{3}$ (By Pascal's rule)

Hence the result is true for $k + 1$

Hence by induction assumption the result is true for all integers $n \geq 2$

Problem 6

For $n \geq 1$,verify that $1^2 + 3^2 + 5^2 + \cdots + (2n - 1)^2 = \binom{2n+1}{3}$

Solution

When $k = 1, 1^2 = 1 = \binom{2(1)+1}{3} = \binom{3}{3} = 1$

Assume that result is true for k and prove it is true for $k + 1$.

Therefore, we have $1^2 + 3^2 + \cdots + (2k - 1)^2 = \binom{2k+1}{3} \ldots . (1)$

Now, $1^1 + 3^2 + \cdots + (2k-1)^2 + [2(k+1) - 1^2]$

$$= 1^2 + \cdots + (2k-1)^2 + (2k+1)^2$$

$$= \binom{2k+1}{3} + (2k+1)^2 \quad \text{by } (1)$$

$$= \frac{(2k+1)!}{3!\,(2k-2)!} + (2k+1)^2$$

$$= \frac{(2k+1)!\,(2k)(2k-1)!}{3!\,(2k-2)!\,(2k)(2k-1)!} + \frac{6(2k+1)^2.\,(2k)!}{6(2k)!}$$

$$= \frac{(2k+1)!\,[(2k)(2k-1) + 6(2k+1)]}{3!\,(2k)!}$$

$$= \frac{(2k+1)!\,[4k! - 2k + 12k + 6]}{3!\,(2k)!}$$

$$= \frac{(2k+1)!\,[(2k+2)(2k+3)]}{3!\,(2k)!}$$

$$= \frac{(2k+3)!}{3!\,(2k+3-3)!} = \binom{2k+3}{3}$$

So, the result is true for $k+1$.

Hence, $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \binom{2n+1}{3}$

Problem 7

Show that, for $n \geq 1$,

$$\binom{2n}{n} = \frac{1.3.5\ \ldots.\ \ (2n-1)}{2.4.6\ \ldots.\ 2n} 2^{2n}$$

Solution

Let $k = 1$ therefore $\binom{2}{1} = \frac{2!}{1!1!} = 2$ and $\frac{1}{2}2^2 = \frac{4}{2} = 2$

Therefore, L.H.S = R.H.S

Assume that the result is true for k and prove it is true for $k+1$

Therefore, we have $\binom{2k}{k} = \frac{1.3.5...(2k-1)}{2.4.6...\ 2k}2^{2k}$

Now, $\binom{2k+2}{k+1} = \frac{(2k+2)!}{(k+1)!(k+1)!}$

$$= \frac{(2k+2)(2k+1)(2k)!}{(k+1)(k+1)k!\,k!}$$

$$= \frac{(2k+2)(2k+1)}{(k+1)(k+1)}\binom{2k}{k}$$

$$= \frac{(2k+2)(2k+1)}{(k+1)(k+1)}.\frac{1.3.5\ ....\ (2k-1)}{2.4.6\ ....\ 2k}2^{2k}$$

$$= \frac{2(k+1)}{(k+1)(k+1)}.\frac{1.3.5\ ....\ (2k-1)(2k+1)}{2.4.6\ ....\ 2k}2^{2k}$$

$$= \frac{2}{(k+1)}.\frac{1.3.5\ ....\ (2k+1)}{2.4.6\ ....\ 2k}2^{2k}$$

$$= \frac{4}{(2k+2)}.\frac{1.3.5\ ....\ (2k+1)}{2.4.6\ ....\ 2k}2^{2k}$$

$$= \frac{1.3.5\ ....\ (2k+1)}{2.4.6\ ....\ (2k)(2k+2)}2^{2k+2}$$

So, the result is true for $k+1$.

Hence, for $n \geq 1$, $\binom{2n}{n} = \frac{1.3.5.....\ (2n-1)}{2.4.6.....\ (2n)}2^{2n}$

Exercise

1. Use problem 5 and the relation $m^2 = 2\binom{m}{2} + m$ for $m \leq 2$, deduce the formula $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

2. Use problem 5 and obtain a proof that

$$1.2 + 2.3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

$$\left[Hint : (m-1)m = 2\binom{m}{2}\right]$$

1.4 Early Number Theory

The number theory originated in a typical way. It can be said that the number theory is one of the very oldest branch of mathematics. It is generally believed that the Greeks depended on the Babylonians and ancient Egyptians to know the properties of the natural numbers. But the beginning of this actual theory brought up by Pythagoras and his disciples.

Pythagoras was born between 580 and 562 BC on the Aegean island of Samos. He had his studies in Egypt and by travelling to Babylonia. After years of wandering, he settled in Croton, in Greek on the heel of the Italian boot, where he found a suitable place for a school. The school concentrated on four ‘mathemata’ or ‘subjects of study’

i) Arithmetica (arith- metic, in the sense of number theory, rather than the art of calculating)

ii) hannonia (music)

iii) geometria (geometry)

iv) astrologia (astronomy).

This fourfold division of knowledge came to be known as the Middle Ages as the quadrivium, along with the trivium of logic, grammar, and rhetoric.

Pythagoras divided his term into two groups.

i) the Pro- bationers (or listeners)

ii) the Pythagoreans. A listener will be promoted to the second class after three years in the first class. The main score discoveries of the school were taught to a student in the second class. The Pythagoreans were a closely united brotherhood, who is bound by an oath not to reveal the founder's secrets. It is said that Pythagorean was drowned in a shipwreck as gods' punishment for boasting that it is he who had added the dodecahedron to the number of regular solids. The Pythagoreans were autocratic and for sometime succeeded in the local government in Croton, but so many of its prominent members died in a revolt in 501 BC. Pythagoreans was also killed and their political influence was destroyed. Yet they continued to exist for at least two more centuries as a philosophical and mathematical society.

In general thesis of the Pythagoreans is that "Everything is Number"; a belief that everything in the universe could only be explained with number and form. The Pythagorean doctrine is a mixture of cosmic philosophy and number mysticism. This writings demonstrated so many things lie 1 for reason, 2 stood for man, 3 for woman, 4 was the Pythagorean symbol for justice, 5 was identified with marriage and so on. The even numbers were capable of separation and so were considered as feminine and earthy. They classified the odd numbers as masculine and divine.

To Pythagoras and his followers, mathematics meant an end of philosophy. The founding School of Alexandria we enter a new phase in which there was a cultivation of mathematics.

At Alexandria, the science of numbers began to develop. Until its destruction by Arabs in 641 A.D., Alexandria stood at the cultural of the Hellenistic world. After its fall, many scholars migrated to Constantinople and this enclave has preserved the mathematical works of various Greek schools. This Alexandrian Museum, brought up the leading poets and scholars of the day. Near to it is an enormous library holding over 700,000 volumes, hand copied. Of them Euclid founder of the School of Mathematics, author of “The Elements” the oldest Greek treatise on mathematics stand in a special class. Euclid is associated with Geometry and three of his books, $VII, VIII,$ and IX, are devoted to number theory.

Next to Bible, Euclid's “Elements” is the widely circulated or studied book. The first printed version appeared in 1482, and sold over a thousand editions. But no actual copy of the words has been found and what remains are the modern editions prepared by Theon of Alexandria, a commentator of the 4^{th} century A.D.

Triangular Number

A number is called triangular if it is the sum of consecutive integers, beginning with 1.

Examples

$1 = 1, 3 = 1 + 2, 6 = 1 + 2 + 3, 10 = 1 + 2 + 3 + 4$

PROBLEMS 1.4

Problem 1

a) A number is triangular if and only if it is of the form $n(n + 1)/2$ for some $n \geq 1$. (Pythagoras, circa 550 B.C.)

b) The integer n is a triangular number if and only if $8n + 1$ is a perfect square. (Plutarch, circa 100 A.D.)

c) The sum of any two consecutive triangular numbers is a perfect square. (Nicomachus, circa 100 A.D.)

d) If n is a triangular number, then so are $9n + 1$, $25n + 3$, and $49n + 6$. (Euler, 1775)

Proof

a) We have $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ ………………… (1)

If X is a triangular number then by the definition for some $n \geq 1$, $X = 1 + 2 + 3 + \cdots + n$

$$X = \frac{n(n+1)}{2} \quad \text{by (1)}$$

b) Assume n is a triangular number, then there is some $k \geq 1$ such that $n = \frac{k(k+1)}{2}$

Therefore, $8n = 8\left[\frac{k(k+1)}{2}\right] = 4k(k+1)$

But $8n + 1 = 4k(k+1) + 1$

$$= 4k^2 + 4k + 1$$

$$= (2k+1)^2$$

Therefore, $8n + 1$ is a perfect square

Conversely, $8n + 1$ is a perfect square then there is an integer k such that $k^2 = 8n + 1$.

Since $8n + 1$ is an odd number we have k is an odd number.

Therefore there is an S such that $k = 2s + 1$.

Which implies $(2s+1)^2 = k^2 = 8n + 1$

Therefore, $4s^2 + 4s + 1 = 8n + 1$

Therefore, $4s(s+1) = 8n$

Therefore, $\frac{s(s+1)}{2} = n$

Therefore, $8n + 1$ is a perfect square implies n is a triangular number.

c) Let $1 + 2 + 3 + \cdots + n = a$.

Since a and b are two consecutive triangular numbers,

We have $1 + 2 + 3 + \cdots + n + (n+1) = b$.

Therefore, $a + b = \frac{n(n+1)}{2} + \frac{n(n+1)}{2} + (n+1)$

$$= n(n+1) + (n+1)$$

$$= (n+1)(n+1)$$

$$= (n+1)^2$$

Therefore $(a+b)$ is a perfect Square.

d) Let $1+2+3+\cdots+k=n$.

Then $9n+1 = 9\left[\frac{k(k+1)}{2}\right]+1$

$$= \frac{9k^2+9k+2}{2}$$

$$= \frac{(3k+1)(3k+2)}{2}$$

$$= \frac{s(s+1)}{2} \text{ Where } 3k+1=s$$

Therefore $9n+1$ is a triangular number.

Now, $25n+3 = 25\left[\frac{k(k+1)}{2}\right]+3$

$$= \frac{25k^2+25k+6}{2}$$

$$= \frac{(5k+2)(5k+3)}{2}$$

$$= \frac{s(s+1)}{2} \text{ Where } 5k+2=s$$

Therefore, $25n+3$ is a triangular number.

Now, $49n+6 = 49\left[\frac{k(k+1)}{2}\right]+6$

$$= \frac{49k^2+49k+12}{2}$$

$$= \frac{(7k+3)(7k+4)}{2}$$

$$= \frac{s(s+1)}{2} \text{ Where } 7k + 3 = s$$

Therefore $49n + 6$ is a triangular number.

Problem 2

If t_n denotes the n^{th} triangular number, Prove that in terms of the binomial coefficients, $t_n = \binom{n+1}{2}$, $n \geq 1$

Proof

Given t_n be the n^{th} triangular number,

Then $t_n = 1 + 2 + 3 + \cdots + n$

Therefore, $t_n = \frac{n(n+1)}{2}$

$$= \binom{n+1}{2}$$

Problem 3

Prove that the square of any odd multiple of 3 is the difference of two triangular numbers; specifically, that $9(2n+1)^2 = t_{9n+4} - t_{3n+1}$.

Solution

Let, t_n be the n^{th} triangular number.

Therefore, $t_n = \frac{n(n+1)}{2}$

Hence, we have $t_{3n+1} = \frac{(3n+1)(3n+2)}{2}$

$$= \frac{9n^2 + 9n + 2}{2}$$

and $t_{9n+4} = \dfrac{(9n+4)(9n+5)}{2}$

$$= \frac{81n^2 + 81n + 20}{2}$$

Therefore,

$$t_{9n+4} - t_{3n+1} = \left(\frac{81n^2 + 81n + 20}{2}\right) - \left(\frac{9n^2 + 9n + 2}{2}\right)$$

$$= \frac{72n^2 + 72n + 18}{2}$$

$$= 36n^2 + 36n + 9$$

$$= 9(4n^2 + 4n + 1)$$

$$= 9(2n + 1)^2$$

Problem 4

Show that the difference between the squares of two consecutive triangular numbers is always a cube.

Solution

Let, t_n denotes the n^{th} triangular number.

Therefore, $t_n = \frac{n(n+1)}{2}$ and $t_{n+1} = \frac{(n+1)(n+2)}{2}$

We have to show that $(t_{n+1})^2 - (t_n)^2 = k^3$, for some integer k.

Now, $(t_{n+1})^2 - (t_n)^2 = \frac{(n+1)^2(n+2)^2 - n^2(n+1)^2}{4}$

$$= \frac{(n + 1)^2[n^2 + 4n + 4 - n^2]}{4}$$

$$= \frac{(n + 1)^2(4n + 4)}{4}$$

$$= (n + 1)^3 \text{ , for } n \geq 1$$

Problem 5

Prove that the sum of the reciprocals of the first n triangular numbers is less than 2; that is,

$$\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\cdots+\frac{1}{t_n}<2\,.$$

Solution

Let, t_n denotes the n^{th} triangular number.

Therefore, $t_n=\frac{n(n+1)}{2}$

Now, $\frac{1}{t_n}=\frac{1}{\frac{n(n+1)}{2}}=\frac{2}{n(n+1)}=2\left[\frac{1}{n}-\frac{1}{n+1}\right]$

Therefore, $\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\cdots+\frac{1}{t_n}$

$$=2\left[\frac{1}{1}-\frac{1}{2}\right]+2\left[\frac{1}{2}-\frac{1}{3}\right]+\cdots+2\left[\frac{1}{n}-\frac{1}{n+1}\right]$$

$$=2\left[\frac{1}{1}-\frac{1}{n+1}\right]$$

$$=2\left(1-\frac{1}{n+1}\right)$$

Since, >0 , Then $n+1>0$, So $\frac{1}{n+1}>0$ and $-\frac{1}{n+1}<0$

Therefore, $1-\frac{1}{n+1}<1$

Which implies, $2\left(1-\frac{1}{n+1}\right)<2$

Therefore, $\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\cdots+\frac{1}{t_n}<2$

Exercise

1. If the triangular number t_n is a perfect square. Prove that $t_{n(n+1)}$ is also a square.

2. In the sequence of triangular numbers two triangular numbers whose sum and difference are also triangular numbers.

CHAPTER - II

2.1 The Division Algorithm

Theorem 2.1 ***Division Algorithm***

Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying $a = qb + r,\ 0 \leq r < b$. The integers q and r are called, respectively, the quotient and remainder in the division of a by b.

Proof

Let a and b are the two integers with $b > 0$.

We begin by proving that the set $S = \{a - xb/x$ is an integer, $a - xb \geq 0\}$ is non empty.

That is, it sufficient to prove that $a - xb$ is non negative.

Because the integer $b \geq 1$, we have $|a|b \geq |a|$, and so $a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$.

For the choice of $x = -|a|$ we have $a - xb \geq 0$, therefore, $a - xb$ lies in S. Hence S is non empty. Then by well ordering property, the set S contains a smallest integer call it as r.

Also by the definition of S, there exists an integer q satisfying $a - qb, 0 \leq r$.

Now we also prove that $r < b$, if not then $r \geq b$ and

$$a - (q + 1)b = (a - qb) - b$$
$$= r - b \geq 0$$

Therefore the integer $a - (q + 1)b$ is belong to the set S. But $a - (q + 1)b = r - b < r$ which is contradiction of the choice of r as the smallest integer of S. Hence $r < b$.

Now to prove the uniqueness:

Let q_1, r_1 be the another pair of integer satisfying $a = q_1 b + r_1, 0 \leq r_1 < b$ ... ... (1)

We have, $a = qb + r, 0 \leq r < b$ ... ... (2)

From (1) and (2) we get, $qb + r = q_1 b + r_1$

then, $qb - q_1 b = r_1 - r$

Which implies $b(q - q_1) = r_1 - r$.

The fact that the absolute value of a product is equal to the product of the absolute value $|r_1 - r| = b|q - q_1|$ ... ... (3) since given that $b > 0$

Adding the two inequalities $-b < -r \leq 0$ and $0 \leq r_1 < b$ or in equivalent term, $|r_1 - r| < b$

$$(3) \Rightarrow \quad b|q - q_1| < b$$

$$|q - q_1| < b/b$$

$$\Rightarrow \quad |\, q - q_1| < 1$$

Which yields $0 \leq |q - q_1| < 1$.

Since, $|q - q_1|$ is a non negative integer, the only possibility is that $|q - q_1| = 0$

This implies $q = q_1$

Therefore substitute, $q = q_1$ in (3)

We get, $|r_1 - r| = 0$

Which implies that, $r_1 - r = 0$

Therefore, $r_1 = r$

Hence the proof.

Corollary 2.2

If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that $a = qb + r$, $0 \leq r < |b|$.

Proof

If $b > 0$ then by theorem 2.1 there exist unique integers q and r such that $a = qb + r,\ 0 \leq r < |b|$ Hence, it is enough to consider the case in which $b < 0$.

If $b < 0$ then $|b| > 0$, then by Theorem 2.1 there exist unique integers q' and r for which $a = q'|b| + r$, $0 \leq r < |b|$.

Note that $|b| = -b$, we may take $q = -q'$ and we get $a = qb + r$, with $0 \leq r < |b|$.

PROBLEMS 2.1

Problem1

Prove that if a and b are integers, with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$

Solution

Given a and b are the two integers with $b > 0$.

By division algorithm, there exists unique integers $q^{'}, r^{'}$ such that $a = q^{'}b + r^{'}, 0 \leq r^{'} < b$

Therefore, $a = q^{'}b + r^{'} + 2b - 2b = (q^{'} - 2)b + r^{'} + 2b$

Let $q = q^{'} - 2\,,\;\; r = r^{'} + 2b$

Therefore r, q are unique.

Since $0 \leq r^{'} < b$, then $2b \leq r^{'} + 2b < b + 2b$ or $2b \leq r < 3b$

Problem 2

Use the Division Algorithm to establish the following:

a) The square of any integer is either of the form $3k$ or $3k + 1$

b) The cube of any integer has one of the form $9k, 9k + 1$ or $9k + 8$

c) The fourth power of any integer is either of the form $5k$ or $5k + 1$

Solution

a) By Division Algorithm, there exists q such that $a = 3q$ or $a = 3q + 1$

Now, $a = 3q$ implies
$$\begin{aligned} a^2 &= 9q^2 \\ &= 3(3q^2) \\ &= 3k \text{ where } k = 3q^2 \end{aligned}$$

Now, $a = 3q + 1$ implies
$$\begin{aligned} a^2 &= (3q + 1)^2 \\ &= 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1 \\ &= 3k + 1 \text{ where } k = 3q^2 + 2q \end{aligned}$$

Therefore, square of any integer is either of the form $3k$ or $3k+1$

b) Let a an integer, then prove that $a^3 = 9k$, $9k+1$ or $9k+8$

Let $a = 3q + r, r = 0,1,2$

Now, $(3q)^3 = 27q^3 = 9(3q^3)$

$$= 9k \text{ where } k = 3q^3$$

Also, $(3q+1)^3 = \binom{3}{0}(3q)^3 + \binom{3}{1}(3q)^2 + \binom{3}{2}3q + \binom{3}{3}$

$$= 27q^3 + 27q^2 + 9q + 1$$

$$= 9(3q^3 + 3q^2 + 9) + 1$$

$$= 9k + 1 \text{ where } k = 3q^3 + 3q^2 + 9$$

Again, $(3q+2)^3 = \binom{3}{0}(3q)^3 + \binom{3}{1}(3q)^2 2 +$

$$\binom{3}{2}(3q)2^2 + \binom{3}{3}2^3$$

$$= 27q^3 + 54q^2 + 36q + 8$$

$$= 9(3q^3 + 6q^2 + 4q) + 8$$

$$= 9k + 8 \text{ where } k = 3q^3 + 6q^2 + 4q$$

Therefore, cube of any integer has one of the form $9k, 9k+1$ or $9k+8$

c) Let n is an integers, to prove that $n^4 = 5k$ or $5k+1$

For that let $n = 5q + r$, $0 \leq r < 5$

Consider $n^4 = (5q + r)^4$

From binomial expansion, each term is a factor of 5 except last term, That is, $\binom{4}{0}(5q)^4 + \binom{4}{1}(5q)^3 r + \binom{4}{2}(5q)^2 r^2$

$$+ \binom{4}{3}(5q)r^3 + r^4$$

If $= 0$, then $r^4 = 0$ and $n^4 = 5k$ as all other term have 5 as a factor.

If $r = 1$, then clearly $n^4 = 5k + 1$

If $r = 2$, then $r^4 = 16 = 15 + 1$, so all terms and 15 have 5 as a factor, so again, $n = 5k + 1$

If $r = 3$, then $r^4 = 81 = 80 + 1$ and $80 = 5 \times 16$, so again, $n^4 = 5k + 1$

Problem 3

For $n \geq 1$, prove that $\frac{n(n+1)(2n+1)}{6}$ is an integer.

Solution

Let $n = 6k + r$, $0 \leq r < 5$ and $A = \frac{n(n+1)(2n+1)}{6}$

If $r = 0$, then $A = k(6k + 1)(12k + 1)$, an integer.

If $r = 1$ then $A = \frac{(6k+1)(6k+2)(12k+3)}{6}$

$$= \frac{(6k+1)(72k^2+42k+6)}{6}$$

$$= (6k + 1)(12k^2 + 7k + 1)\text{, an integer}$$

If $r = 2$ then $A = \frac{(6k+2)(6k+3)(12k+5)}{6}$

$$= \frac{\left(36k^2+30k+6\right)(12k+5)}{6}$$

$= (6k^2 + 5k + 1)(12k + 5)$, an integer

If $r = 3$ then, $A = \frac{(6k+3)(6k+4)(12k+7)}{6}$

$$= \frac{(36k^2 + 42k + 12)(12k + 7)}{6}$$

$= (6k^2 + 7k + 2)(12k + 7)$, an integer

If $r = 4$, $A = \frac{(6k+4)(6k+5)(12k+9)}{6}$

$$= \frac{\left(72k^2+102k+36\right)(6k+5)}{6}$$

$= (12k^2 + 17k + 6)(6k + 5)$, an integer

If $r = 5$, $A = \frac{(6k+5)(6k+6)(12k+11)}{6}$

$$= \frac{(36k^2+66k+30)(12k+11)}{6}$$

$= (6k^2 + 11k + 5)(12k + 11)$, an integer.

Problem 4

If n is an odd integer, show that $n^4 + 4n^2 + 11$ is of the form $16k$

Solution

Let $n = 2k + 1$

Now, $n^4 + 4n^2 + 11 = (n^2 + 2)^2 + 7$

$$= [(2k+1)^2+2]^2+7$$

$$= [4k^2+4k+1+2]^2+7$$

$$= (4k^2+4k+3)^2+7$$

$$= 16k^4+16k^3+12k^2+16k^3+16k^2$$

$$+12k+12k^2+12k+9+7$$

$$= 16k^4+32k^3+40k^2+24k+16$$

We know that k is of the form $k = 2q$ or $2q+1$

When $k = 2q$ then,

$$n^4+4n^2+11 \;=\; 16(2q)^4+32(2q)^3+40(2q)^2$$

$$+24(2q)+16$$

$$= 16[(2q)^4+2(2q)^3+10q^2+3q+1]$$

$= 16k$, Where $k = (2q)^4+2(2q)^3$

$$+10q^2+3q+1$$

When $k = 2q+1$, then,

$$n^4+4n^2+1 = 16(2q+1)^4+32(2q+1)^3+40(2q+1)^2$$

$$+24(2q+1)+16$$

$$= 16(2q+1)^4+32(2q+1)^3+160q^2$$

$$+160q+40+40q+24+16$$

$$= 16[(2q+1)^4+2(2q+1)^3+10q^2$$

$$+10q+3q+4+1]$$

$$= 16[(2q+1)^4+2(2q+1)^3+10q^2$$

$$+10q+3q+5]$$

$= 16k$, where $k = (2q+1)^4+2(2q+1)^3$

$$+10q^2 + 10q + 3q + 5$$

Problem 5

Prove that the square of any odd integer is of the form $8k + 1$

Solution

By the division algorithm, any integer can be represented as one of the forms $4q, 4q + 1, 4q + 2, 4q + 3$

Among the integers $4q + 1, 4q + 3$ are odd.

Therefore, $(4q + 1)^2 = 16q^2 + 8q + 1$

$= 8(2q^2 + q) + 1$

$= 8k + 1$ where $k = 2q^2 + q$

Also, $(4q + 3)^2 = 16q^2 + 24q + 9$

$= 16q^2 + 24q + 8 + 1$

$= 8(2q^2 + 3q + 1) + 1$

$= 8k + 1$, where $k = 2q^2 + 3q + 1$

Problem 6

Show that the expression $\frac{a(a^2+2)}{3}$ is an integer.

Solution

According to the division algorithm, every integer 'a' is of the form $3q, 3q + 1, 3q + 2$

When $a = 3q$, then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3}$

$= \frac{3q(9q^2 + 2)}{3}$

$= q(9q^2 + 2)$ which is an integer

When $a = 3q + 1$, then $\frac{a\left(a^2+2\right)}{3} = \frac{(3q+1)\left[(3q+1)^2+2\right]}{3}$

$$= \frac{(3q + 1)[(9q^2 + 6q + 1) + 2]}{3}$$

$$= \frac{(3q + 1)3(3q^2 + 2q + 1)}{3}$$

$= (3q + 1)(3q^2 + 2q + 1)$ which is an integer

When $a = 3q + 2$, then $\frac{a\left(a^2+2\right)}{3} = \frac{(3q+2)\left[(3q+2)^2+2\right]}{3}$

$$= \frac{(3q + 2)[(9q^2 + 12q + 4) + 2]}{3}$$

$$= \frac{(3q + 2)[9q^2 + 12q + 6]}{3}$$

$$= \frac{(3q + 2)3(3q^2 + 4q + 2)}{3}$$

$= (3q + 2)(3q^2 + 4q + 2)$ which is an integer

Exercise Problems

1) Show that any integer of the form $6k + 5$ is also of the form $3j + 2$ but not conversely.

2) Prove that $3a^2 - 1$ is never a perfect square.

3) Show that the cube of any integer is of the form $7k$ or $7k \pm 1$

4) For $n \geq 1$, establish that the integer $n(7n^2 + 5)$ is of the form $6k$

2.2 The Greatest Common Divisor

Definition

An integer b is said to be divisible by an integer a, $a \neq 0$ in symbols $a|b$,if there exist some integer c such that $b = ac$.

We write $a \nmid b$ to indicate that b is not divisible by a.

Example

1) 12 is divisible by 4, because $12 = 4 \times 3$

2) 10 is not divisible by 3

Theorem 2.3

For integers a, b, c, the following hold:

a) $a \mid 0$, $1 \mid a$, $a \mid a$.

b) $a \mid 1$ if and only if $a = \pm 1$.

c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

d) If $a \mid b$ and $b \mid c$, then $a \mid c$.

e) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.

f) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

g) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.

Proof

a) We have, $a \times 0 = 0$ therefore, $|0$.

Also, we have, $a \times 1 = a$ and $1 \times a = a$

Therefore, $1|a$ and $a \mid a$.

b) Assume that $a|1$ then $a.c = 1$ for some c

Suppose $|c| \neq 0$ then $|c| > 1$.

By the definition we have $|a| \geq 1$.

Therefore, $|a||c| > 1$.

Which is contradiction to $a.c = 1$.

Therefore, $|c| = 1 \Longrightarrow c = \pm 1$.

If $c = 1$ then $ac = a = 1 \Longrightarrow a = 1$.

If $c = -1$ then $ac = -a = 1 \Longrightarrow a = -1$.

Therefore, $a = \pm 1$.

Conversely, assume that $a = \pm 1$.

If $a = 1$ then $a.1 = 1 \Longrightarrow a|1$.

If $a = -1$ then $a.(-1) = 1 \Longrightarrow a|1$.

c) If $a|b$, then there exists an integer e such that, $b = ae$ and if $c|d$, then there exists an integer f such that $d = cf$

To prove $ac|bd$

Consider $bd = ae.cf$

$$= (ac).(ef)$$

This implies $ac|bd$.

d) If $a|b$ then there exist an integer d such that $b = ad$ and if $b|c$ then there exist an integer e such that $c = be$

To prove $a|c$.

Consider $c = be$

$$= ade$$

Therefore, $c = a(de)$

This implies $a|c$

e) Assume that $a|b$ and $b|a$.

Now, $a|b \Longrightarrow b = ax$ for some x and $b|a$

$\Longrightarrow a = by$ for some y

Therefore, $a = (ax)y \Longrightarrow 1 = xy \Longrightarrow x|1$.

Therefore, we get $x = \pm 1$.

If $x = 1$ then $ax = b$ implies $a = b$.

If $x = -1$ then $ax = b$ implies $a = -b$

Therefore, $a = \pm b$.

Conversely, assume that $a = \pm b$.

If $a = b$ then $a.1 = a = b$ then $a|b$ and

$b.1 = b = a$ then $|a$.

If $a = -b$ then $a(-1) = (-b)(-1) = b$ then $a|b$

and $b(-1) = -b = a$ then $b|a$.

Therefore, if $a = \pm b$ then $a \mid b$ and $b \mid a$

f) If $a|b$ then there exists an integer c such that $b = ac$

Also given, $b \neq 0$ implies that $c \neq 0$

Taking absolute values we get $|b| = |ac|$

$$\Longrightarrow \quad |b| = |a||c|$$

Because $c \neq 0$ it follows that $|c| \geq 1$,then we have, $|b| \geq |a|$.

Therefore $|a| \leq |b|$.

g) If $a|b$ then there exist an integer p such that $b = ap$ also if $a|c$ then there exist an integer q such that $c = aq$

To prove $a|(bx + cy)$

Consider, $bx + cy = (ap)x + (aq)y$

$$= a(px + qy)$$

Therefore, $a|(bx + cy),$ where $px + qy$ is an integer.

Definition

Let a and b be given integers with at least one of them different from zero. The greatest common divisor of a and b denoted by $gcd(\mathrm{a}, \mathrm{b})$, is the positive integer d satisfying the following

$i)$ $d|a$ and $d|b$

$ii)$ If $c|a$ and $c|b$ then $c|d$, $c \leq d$

Example

Find $\mathrm{gcd}(-12{,}30)$

Solution

The positive divisors of -12 are $1{,}2{,}3{,}4{,}6{,}12$. And the positive divisor of 30 are $1{,}2{,}3{,}5{,}6{,}10{,}15{,}30$.

The positive common divisor of -12 and 30 are $1{,}2{,}3{,}6$

Here 6 is the largest of these integers.

Therefore, $\mathrm{gcd}(-12{,}30) = 6$

Theorem 2.4

Given integers a and b not both of which are zero, there exist integers x and y such that $\mathrm{gcd}(\mathrm{a}, \mathrm{b}) = ax + by$.

Proof

Consider the set S of all positive linear combination of a and b that is, $S = \{au + bv/au + bv > 0, u, v$ are integers$\}$.

Since integers a and b not both of which are zero we have the set S is a non empty set.

Therefore, by well ordering principle S has a least element say d, then, there exists an integer x and y such that $d = ax + by$.

We claim that $d = gcd(a, b)$

By division algorithm, there exists an integers q and r such that $a = qd + r, 0 \leq r < d$ ... ... (1)

$\Rightarrow \quad r = a - qd$

$= a - q(ax + by)$

$= a - qax - qby$

$= a(1 - qx) + b(-qy)$

If r were positive, then this representation would imply that r is the member of S. Which is contradiction, because d is the least element in S.

Therefore, $r = 0$ Hence (1) implies $a = qd \Rightarrow \quad d|a$

Similarly, $b = qd + r$

Since $r = 0, \; b = qd \;\Rightarrow\; d|b$

Therefore d is the common divisor of a and b ... ... (2)

If c is the arbitrary common divisor of the integers a and b.

That is, $c|a$ and $c|b$ then to prove $c|d, \; c \leq d$

Since, $c|a$ and $c|b$, we have $c|(ax + by) = c|d$ by result of the theorem 2.3 we have $|c| \leq |d|$, therefore, $c \leq d$

Therefore, we have if $c|a$ and $c|b$ then $c|d$ and $c \leq d$….. (3)

From (2) and (3), d is the greatest common divisor of a and b.

Therefore, $gcd(a, b) = d$

Hence, $gcd(a, b) = ax + by$

Corollary 2.5

If a and b are given integers not both zero then the set $T = \{ax + by | x, y$ are integers$\}$ is precisely the set of all multiples of $d = gcd(a, b)$.

Proof

Given $T = \{ax + by | x, y$ are integers$\}$

Assume $d = gcd(a, b) \implies d|a$ and $d|b$

Therefore, we have $d|(ax + by)$ for the integers x and y. Thus every member of T is a multiple of d.

Conversely, we write $d = ax_0 + by_0$ for suitable integers x_0 and y_0, so that, any multiple nd is of the form $nd = n(ax_0 + by_0) = anx_0 + bny_0$

Hence nd is a linear combination of a and b

Therefore, it is lies in T.

Definition

Two integers a and b not both of which are zero, are said to be relatively prime whenever, $gcd(a, b) = 1$.

Example

$gcd(2,5) = 1$, then 2 and 5 are relatively prime.

Theorem 2.6

Let a and b be integers not both zero, then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Proof

Assume that a and b are relatively prime.

Since a and b are relatively prime then $gcd(a, b) = 1$

By the above result there exist an integer x and y satisfies $1 = ax + by$

Conversely, assume that $1 = ax + by$ for some choice of x and y and that $d = gcd(a, b)$ … … … … (1)

Now, $gcd(a, b) = d$, implies that $d|a$ and $d|b$

Therefore, $d|(ax + by)$.

$\Longrightarrow \quad d|1 \qquad$ [since $1 = ax + by$]

Therefore, $d = \pm 1$

Since d is a positive integer we have $d = 1$

Therefore (1) $\Longrightarrow gcd(a, b) = 1$

Therefore, a and b are relatively prime.

Corollary 2.7

If $a|c$ and $b|c$ with gcd$(a,b) = 1$ then $ab|c$

Proof

If $a|c$ there exist an integer r such that $c = ra$ and if $b|c$ there exist an integer s such that $c = bs$.

Also $gcd(a,b) = 1$, we can write $1 = ax + by$ for some choice of x and y

Multiply the above relation by c on both sides

we get, $acx + bcy = c$

$\Longrightarrow \quad a(bs)x + b(ra)y = c$

$\Longrightarrow \quad absx + abry = c$

$\Longrightarrow \quad ab(sx + ry) = c$

Therefore, $ab|c$ [by divisibility theorem]

Corollary 2.8

If gcd$(a,b) = d$ then gcd$(a/d\ , b/d) = 1$

Proof

We observe that a/d and b/d are integers because d is the division of both a and b

Now, knowing that gcd$(a,b) = d$

It is possible to find integers x and y such that $d = ax + by$

Dividing the above equation we obtain the expression

$$1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y$$

Since a/d and b/d are integers, the conclusion is that a/d and b/d are relatively prime.

Therefore, $gcd(\mathrm{a/d}\,, b/d) = 1$

Theorem 2.9 ***Euclid's lemma***

If $a|bc$ with $gcd(a,b) = 1$, then $a|c$

Proof

Given $a|bc$ with $gcd(a,b) = 1$

Then, by Theorem 2.6, we have $1 = ax + by$, where x and y are integers.

Multiply by c we get, $c = 1.c = (ax + by)c = acx + bcy$

We have, $a|bc$ and $a|ac$ also.

Hence, $a|(acx + bey)$.

That is, $a|c$

Theorem 2.10

Let a, b be integers, not both zero.

For a positive integer d, $d = gcd(a,b)$ if and only if

a) $d|a$ and $d|b$

b) Whenever $c|a$ and $c|b$, then $c|d$

Proof

Assume, $d = gcd(a,b)$, then, $d|a$ and $d|b$

By the Theorem 2.4, d is expressible as $d = ax + by$ for some integers x, y.

Thus, if $c|a$ and $c|b$, then $c|(ax + by)$, or $c|d$

Conversely, let d be any positive integer satisfying the stated conditions.

Since we have, $c|a$ and $c|b$, then $c|d$ implies that $d \geq c$ and hence we conclude that d is the greatest common divisor of a and b

That is $d \ = \ gcd(a, b)$

PROBLEMS 2.2

Problem 1

If $a|b$, show that $(-a)|b$, $a|(-b)$ and $(-a)|(-b)$

Solution

Given $a|b$, then there exists c such that $a. c = b$

Now, $a. c = (-a). (-c) = b$ implies that (– $a)|b$

Also – $(a. c) = -b = a. (-c)$ implies that $a|(-b)$

Also since we have $a. c = b$

$\Longrightarrow -(a. c) = -b$

$\Longrightarrow (-a). c = -b$ implies that $(-a)|(-b)$

Problem 2

Given integers a, b, c, d verify the following:

a) If $a|b$ then $a|bc$

b) If $a|b$ and $a|c$, then $a^2|bc$

c) $a|b$ if and only if $ac|bc$, where $c \neq 0$

Solution

a) If $a|b$ then there exists an integer x such that $ax = b$.Therefore we have $axc = bc$.

This implies that $a|bc$

b) If $a|b$ then there exists an element x such that $ax = b$ and if $a|c$ then there exists an element y such that $ay = c$.

Therefore $(ax)(ay) = bc = a^2xy$

This gives $a^2|bc$

c) If $a|b$ then there exists x such that $ax = b$ therefore we have $acx = bc$

This implies that $ac|bc$

Conversely, If $ac|bc$ then there exists x such that $acx = bc$.

Since $c \neq 0$, we have $ax = b$

Which implies that $a|b$

Problem 3

Prove that for any integer a, one of the integers $a, a + 2, a + 4$ is divisible by 3

Solution

Case (i) Suppose $3 \nmid a$

Then we have $a = 3q_1 + 1$ or $3q_2 + 2$

Suppose $a = 3q_1 + 1$, then $a + 2 = 3q_1 + 3 = 3(q_1 + 1)$

So, $3|(a + 2)$

Suppose $a = 3q_2 + 2$, then $a + 4 = 3q_2 + 6 = 3(q_2 + 2)$

So, $3|(a + 4)$

Case (ii) Suppose $3 \nmid a + 2$

Therefore $a + 2 = 3q_1 + 1$ or $a + 2 = 3q_2 + 2$

Suppose $a + 2 = 3q_1 + 1$, then $a = 3q_1 - 1$

So $a + 4 = 3q_1 + 3 = 3(q_1 + 1)$

Therefore $3|(a + 4)$

Suppose $a + 2 = 3q_2 + 2$, then $a = 3q_2$, so $3|a$

Case (iii) Suppose $3 \nmid (a + 4)$

Therefore we have $a + 4 = 3q_1 + 1$ or $3q_2 + 2$

Suppose $a + 4 = 3q_1 + 1$, then $a = 3q_1 - 3$, so $3|a$

Suppose $3q_2 + 2$, then $a = 3q_2 - 2\,, a + 2 = 3q_2$

Therefore $3|(a + 2)$

Problem 4

Prove that if a and b are both odd integers, then $16\,|(a^4 + b^4 - 2)$.

Solution

Let $a = 2r + 1$ and $b = 2s + 1$

Now,

$$\begin{aligned} a^4 &= (2r + 1)^4 \\ &= 24r^4 + 4c_1(2r)^3 + 4c_2(2r)^2 + 4c_3(2r) + 1 \\ &= 16\,r^4 + 32\,r^3 + 24\,r^2 + 8r + 1 \end{aligned}$$

Therefore $a^4 + b^4 - 2 \ = 16\,r^4 + 32\,r^3 + 24\,r^2 + 8r$

$$+16s^4 + 32s^3 + 24s^2 + 8s$$

All terms divisible by 16 except perhaps $24r^2 + 8r, 24s^2 + 8s$

But if r is even, then $r = 2w$ for some w and therefore,

$24\,r^2 + 8r = \ 96w^2 + 16w$ which is divisible by 16.

If r is odd, then $r = 2w + 1$ for some w

Therefore $24r^2 + 8r \ = 24(2w + 1)\ + 8(2w + 1)$

$$= 96w^2 + 96w + 24 + 16w + 8$$

$$= 96w^2 + 96w + 16w + 32$$

Which is divisible by 16.

Similarly, for $24s^2 + 8s$, which is also divisible by 16.

Therefore $16|a^4 + b^4 - 2$.

Problem 5

Given an odd integer a, establish that $a^2 + (a + 2)^2 + (a + 4)^2 + 1$ is divisible by 12.

Solution

Let $a = 2n + 1$

Therefore, $(2n + 1)^2 + \ (2n + 3)^2 + \ (2n + 5)^2 + 1$

$$= 4n^2 + 4n + 1 + 4n^2 + 12n + 9$$

$$+4n^2 + 20n + 25 + 1$$

$$= 12n^2 + 36n + 36$$

$$= 12(n^2 + 3n + 3)$$

Therefore, $12|(2n + 1)^2 + \ (2n + 3)^2 + \ (2n + 5)^2 + 1$

That is $12|a^2 + (a + 2)^2 + \ (a + 4)^2 + 1$

Problem 6

Prove that the expression $(3n)!/(3!)^n$ is an integer for all $n \geq 0$.

Solution

We prove this result by induction method.

When $n = 1$,

Then $3!/3! = 1$, is an integer

Assume that the result is true when $n = k$.

That is, $(3k)!/(3!)^k = l$ is an integer.

Next to prove this result for $n = k + 1$

Now, $[3(k + 1)]!/(3!)k + 1 \ = (3k + 3)!/\ (3!)k(3!)$

$$= \frac{(3k + 3)(3k + 2)(3k + 1)(3k)!}{3 \times 2 \times 1 \times (3!)^k}$$

$$= \frac{3(k + 1)(3k + 2)(3k + 1) \times l}{3 \times 2 \times 1}$$

$$= \frac{(k + 1)(3k + 2)(3k + 1) \times l}{2}$$

If k is odd, then $k + 1$ is even ,

So, $(k + 1)/2 \ = \ x$, for some integer x

If k is even , then $3k + 2$ is even ,

So $(3k + 2)/2 \ = \ x$, for some integer x

Therefore, entire expression is an integer.

Problem 8

Establish that the difference of two consecutive cubes is never divisible by 2.

Solution

Let a^3 and $(a+1)^3$ are the two consecutive cubes.

We have to show that $(a+1)^3 - a^3$ never divisible by 2

Suppose a is even then $a = 2n$.

Therefore, $(a+1)^3 - a^3 = (2n+1)^3 - (2n)^3$

$$= 8n^3 + 12n^2 + 6n + 1 - 8n^3$$

$$= 2(6n^2 + 3n) + 1$$

$$= 2k + 1 \text{ where } k = 6n^2 + 3n$$

Which is odd. Hence $(a+1)^3 - a^3$ never divisible by 2.

Suppose a is odd then $a = 2n + 1$.

Therefore, $(a+1)^3 - a^3 = (2n+2)^3 - (2n+1)^3$

$$= (8n^3 + 24n^2 + 12n + 8)$$

$$-(8n^3 + 12n^2 + 6n + 1)$$

$$= 12n^2 + 6n + 7$$

$$= 12n^2 + 6n + 6 + 1$$

$$= 2(6n^2 + 3n + 3) + 1$$

$$= 2k + 1 \text{ where } k = 6n^2 + 3n + 3$$

Which is odd. Hence $(a+1)^3 - a^3$ never divisible by 2.

Problem 10

For a nonzero integer a, show that

a) $gcd(a,0) = |a|$

b) $gcd(a,a) = |a|$

Solution

a) From theorem 2.3 (a) we have $a|0$ and $a|a$ therefore $|a|$ is the common divisor of a and 0.

Let c be an another common divisor of a and 0.

Since a is a nonzero integer we have a is the greatest common divisor of a and 0.

Therefore, $c|a$ then by theorem 2.3 (f) $|c| \leq |a|$.

Therefore, $|a|$ is the greatest common divisor of a and 0.

Which implies $gcd(a, 0) = |a|$

b) From theorem 2.3 (a) we have $a|a$ therefore $|a|$ is the common divisor of a and a.

Let c be an another common divisor.

But, a is the greatest common divisor of a and a.

Therefore, $c|a$ then by theorem 2.3 (f) $|c| \leq |a|$.

Therefore, $|a|$ is the greatest common divisor of a and a.

Which implies $gcd(a, a) = |a|$

2.3 The Euclidean Algorithm

The greatest common divisor of two integers can be found by listing all the positive divisors and choosing the largest one common to each. But this is difficult for large number. Here Euclidean Algorithm is used to find the gcd of two integers.

The Euclidean Algorithm may be described as follows:

Theorem 2.9

Let a and b be two integers whose greatest common divisor is desired.

Proof

Let a & b be two integers.

Since, $gcd(|a|\,,|b|) = gcd\ \ (a,b)$, there is no harm in assuming that $a \geq b > 0$.

The first step is to apply the division algorithm a & b, we get $a = q_1\, b + r_1\,, 0 \leq r_1 < b$

If it happens that $r_1 = 0$, then $a = q_1\, b$

Which implies $b|a$ and $gcd\ \ (a\,,b) = b.$

When $r_1 \neq 0$ divide b by r_1 to produce the integer q_1 and r_1 satisfying $b = q_2\ r_1 + r_2\,,\ 0 \leq r_2 < r_1$

If $r_2 = 0$ we stop, otherwise proceed as before to obtain $r_1 = q_3 r_2 + r_3, 0 \leq r_3 < r_2$

If $r_3 = 0$ than we stop, otherwise proceed as before to obtain $r_2 = q_4 r_3 + r_4, 0 \leq r_4 < r_3$

This division process continues until some zero remainder appears , say at the $n + 1$ stage r_{n-1} is divided by r_n.

The result is the following system of equations:

$$a = q_1 b + r_1, \quad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \;\; 0 < r_3 < r_2$$

$$r_2 = q_4 r_3 + r_4, \;\; 0 < r_4 < r_3$$

$$\begin{matrix} . & . & . \\ . & . & . \\ . & . & . \end{matrix}$$

$$r_{n-2} = q_n r_{n-1} + r_n, 0 < r_4 < r_3$$

$$r_{n-1} = q_{n+1} r_n + 0$$

We argue that r_n , the last nonzero remainder that appear in this manner which is equal to $gcd\ (a\ ,b)$.

Lemma 2.10

If $a = qb + r$, then $gcd(a, b) = gcd(b, r)$.

Proof

Given $a = qb + r$

If $d = gcd(a, b)$, then we have $d|a$ and $d|b$.

Which will imply that $d\ |(a - qb)$, or $d|\ r$.

Thus, d is a common divisor of both b and r.

Claim, d is a greatest common divisor of both b and r

If c is an arbitrary common divisor of b and r, then $c|(qb + r)$.

Hence $c|a$.

This makes c a common divisor of a and b, so that $c \leq d$.

Hence, d is a greatest common divisor of both b and r.

Therefore, $d = gcd(b, r)$

$\Longrightarrow gcd(a, b) = gcd(b, r)$

Example 1

Find $gcd(12378, 3054)$.

Solution

By Division Algorithm we have, $a = qb + r$

Here $a = 12378, b = 3054$

Therefore, $12378 = 4.3054 + 162$

$3054 = 18.162 + 138$

$162 = 1.138 + 24$

$138 = 5.24 + 18$

$24 = 1.18 + 6$

$18 = 3.6 + 0$

Hence by Euclidean Algorithm, the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

Therefore, $6 = gcd(12378, 3054)$

Example 2

Use the Euclidean algorithm to obtain integers x and y satisfy $gcd(12378, 3054) = 12378x + 3054y$.

Solution

Since, $gcd(12378, 3054) = 6$,we represent 6 as a linear combination of the integers 12378 and 3054.

We have, $6 = 24 - 18$

$= 24 - (138 - 5.24)$

$$= 6.24 - 138$$

$$= 6(162 - 138) - 138$$

$$= 6\,.\,162 - 7\,.\,138$$

$$= 6.162 - 7(3054 - 18.162)$$

$$= 132.162 - 7.3054$$

$$= 132(12378 - 4.3054) - 7.3054$$

$$= 132\,.\,12378 + (-535)3054$$

Therefore, $6 = gcd(12378, 3054) = 12378x + 3054y,$ where $x = 132$ and $y = -535.$

Note that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054; among other possibilities, we could add and subtract 3054.12378 to get $6 = (132 + 3054)12378 + (-535 - 12378)3054$. Therefore, $6 = 3186.12378 + (-12913)3054$

Note

The French mathematician Gabriel Lame (1795-1870) proved that the number of steps required in the Euclidean Algorithm is at most five times the number of digits in the smaller integer.

Theorem 2.11

If $k > 0$, then $gcd(ka, kb) = k\ gcd(a, b)$

Proof

If each of the equations appearing in the Euclidean algorithm for a and b is multiplied by k.

We obtain $ak = q_1bk + r_1k$,$0 < r_1k < bk$

$$bk = q_2r_1k + r_2k \text{ ,} 0 < r_2k < r_1k$$

$$r_1k = q_3r_2k + rr_3k \text{ ,} 0 < r_3k < r_2k$$

$$r_2k = q_4r_3k + r_4k \text{ ,} 0 < r_4k < r_3k$$

. . .

. . .

. . .

$$r_{n-2}k = q_nr_n - 1 + r_nk \text{ ,} 0 < r_nk < r_{n-1}k$$

$$r_{n-1}k = q_{n+1}r_nk + 0$$

This is clearly the Euclidean algorithm apply to the integer ak and bk.

So that their gcd is the last non zero remainder r_nk.

That is; $gcd(ka, kb) = r_nk = k\ gcd(a, b)$

Therefore, $gcd(ka, kb) = k\ gcd(a, b)$.

Corollary 2.12

For any integer $k \neq 0$, $gcd(ka, kb) = |k|gcd(a, b)$

Proof

It is sufficient to consider the case in which $k < 0$ then, $-k = |k| > 0$

And by theorem 2.11, $gcd(ka, kb) = gcd(-ka, -kb)$

$$= gcd(|k|a, |k|b)$$

$$= |k|gcd(a, b)$$

Therefore, $gcd(ka, kb) = \left|k\right| gcd(a, b)$

Example 2.4

We see that,
$$\begin{aligned} gcd(12{,}30) &= gcd(2 \times 6\ {,}2 \times 15) \\ &= 2\ gcd(6{,}15) \\ &= 2\ gcd(3 \times 2\ {,}3 \times 5) \\ &= 2 \times 3\ gcd(2{,}5) \\ &= \ 2 \times 3\ = 6 \end{aligned}$$

Least common multiple

The least common multiple of two non zero integers a and b denoted by $lcm(a, b)$ is the positive integer m satisfying the following:

(i) $a|m$ and $b|m$

(ii) If $a|c$ and $b|c$ with $c > 0$, then $m \leq c$

Theorem 2.13

For any positive integer a and b, $gcd(a, b). lcm(a, b) = ab.$

Proof

To begin the proof, put $d = gcd(a, b)$

Therefore, d is the common divisor of a and b, that is $d|a$ and $d|b$

If $d|a$ there exists an integer r such that $a = dr$

If $d|b$ there exists an integer s such that $b = ds$

Let $m = \dfrac{ab}{d}$

Therefore, m is the common multiple of a and b, that is $a|m$ and $b|m$

If $a|m$ there exists an integer s such that $m = as$

If $b|m$ there exists an integer r such that $m = rb$

Now, let c be any positive integer that is an common multiple of a and b.

If $a|c$ there exists an integer u such that $c = au$

If $b|c$ there exists an integer v such that $c = bv$

As we know there exists an integer x and y satisfying $d = ax + by$

In consequence, $\frac{c}{m} = \frac{c}{\left(\frac{ab}{d}\right)}$

$$= \frac{cd}{ab}$$

$$= \frac{c(ax + by)}{ab}$$

$$= \frac{cax}{ab} + \frac{cby}{ab}$$

$$= \left(\frac{c}{a}\right)x + \left(\frac{c}{a}\right)y$$

$$= vx + uy$$

$$c = m(vx + uy)$$

Therefore, $m|c$

Hence, we conclude that $c \geq m$

By definition $lcm\,(a, b) = m$

$lcm\ (a,b)\ = m = \frac{ab}{d}$

$lcm\ (a,b).d\ =\ ab$

Therefore, $lcm\ (a,b)gcd(a,b)\ = ab$

Corollary 2.14

For any choice of positive integer $lcm\ (a,b) = ab$ if and only if $gcd(a,b) = 1$

Note

In case of three integers a,b,c not all zero $gcd(a,b,c)$ is defined to be the positive integer d having the following properties:

a) d is the divisor of a,b and c

b) If e divides the integer a,b,c then $e \leq d$

Example : $gcd(39,42,54)\ =\ 3$

PROBLEMS 2.3

Problem 1

Find $gcd(143,227)$

Solution

By division algorithm, we have $a = qb + r$

Here $a = 227, b = 143$

Therefore, $227 = 1(143) + 84$

$143 = 1(84) + 59$

$84 = 1(59) + 25$

$$59 = 2(25) + 9$$

$$25 = 2(9) + 7$$

$$9 = 1(7) + 2$$

$$7 = 3(2) + 1$$

$$2 = (2)1 + 0$$

Therefore, $gcd\ (143{,}227) = 1$

Problem 2

Find $i)gcd(306{,}657)$

$ii)gcd(272{,}1479)$

Solution

i) We have, $657 = 2.306 + 45$

$$306 = 6.45 + 36$$

$$45 = 1.36 + 9$$

$$36 = 4.9 + 0$$

Therfore, $gcd(306{,}657) = 9$

ii) We have, $1479 = 5.272 + 119$

$$272 = 2.119 + 34$$

$$119 = 3.34 + 17$$

$$34 = 17.2 + 0$$

Therefore, $gcd(272{,}1479) = 17$

Problem 3

Use the Euclidean algorithm to obtain integers x and y satisfying the following

a) $gcd(56,72) = 56x + 72y$

b) $gcd(24,138) = 24x + 138y$

Solution

a) We have, $72 = 1.56 + 16$

$56 = 3.16 + 8$

$16 = 2.8 + 0$

Hence, $gcd(56,72) = 8$

Therefore, $8 = 56 - 3.16$

$= 56 - 3(72 - 56)$

$= (4)56 - (3)72$

$= 56(4) + 138(-72)$

b) We have, $138 = 5.24 + 18$

$24 = 1.18 + 6$

$18 = 3.6 + 0$

Hence, $gcd(24,138) = 6$

Therefore, $6 = 24 - 18$

$= 24 - (138 - 5.24)$

$= (6)24 - 138$

$= 24(6) + 138(-1)$

Problem 4

Find a) $lcm(143,227)$ b) $lcm(306,657)$

Solution

a) First, find the $gcd(143,227)$

We have, $227 = 1.143 + 84$

$$143 = 2.84 + 25$$

$$84 = 3.25 + 9$$

$$25 = 2.9 + 7$$

$$9 = 7 + 2$$

$$7 = 3.2 + 1$$

Hence, $gcd(143,227) = 1$

Therefore $lcm\ (143,227) = 143 \times 227 = 32461$

b) First, find the $gcd(306,657)$

We have, $657 = 2.306 + 45$

$$306 = 7.45 - 9$$

$$45 = 5.9 + 0$$

Therefore, $gcd(306,657) = 9$

Therefore, $lcm(306,657) = \frac{(306\times 657)}{9} = 22338$

Problem 5

Find integer x, y, z satisfying $gcd(198,288,512) = 198x + 288y + 512z$

Solution

We Know that, $gcd(198,288,512) = gcd(gcd(198,288),512)$

Now, $288 = 198 + 90$

$$198 = 2.90 + 18$$

$$90 = 5.18 + 0$$

Hence $gcd(198,288) = 18$

Also, $18 = 198 - 2.90$

$$= 198 - 2(288 - 198)$$

$$= (-2).288 + 3.198$$

Now for, gcd $(18{,}512)$

We have, $512 = 28.18 + 8$

$$18 = 2.8 + 2$$

$$8 = 4.2$$

Therefore, $gcd(18{,}512) = 2$

Which gives gcd $(198{,}288{,}512) = 2$

Also, $2 = 18 - 2.8$

$$= 18 - 2(512 - 28.18)$$

$$= 57.18 - 2.512$$

$$= 57(3.198 - 2.288) - 2.512$$

$$= 171(198) - 114(288) - 2.512$$

Therefore, $x = 171$; $y = -114$; $z = -2$

2.4 The Diophantine Equation $ax + by = c$

The simplest type of Diophantine Equation that we shall consider the line Diophantine equation with two unknown $ax + by = 0$ where a, b, c are integers and a, b not both zero.

The solution of this equation is the pair of integers x_0, y_0 that when substituted into the equation satisfying it; that is, $ax_0 + by_0 = c$

Theorem 2.15

The liner Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other Solutions are given by $x = x_0 + \left(\frac{b}{d}\right)t$, $y = y_0 - \left(\frac{a}{d}\right)t$ where t is an arbitrary integer.

Proof

Assume that the liner Diophantine equation has a solution.

To prove, $d|c$ where $d = gcd(a, b)$

Now, $d = gcd(a, b)$ implies that $d|a$ and $d|b$

Therefore, there exist an integer r and s such that $a = dr, b = ds$

If the solution of $ax + by = c$ exist, so that $ax_0 + by_0 = c$ for some suitable x_0,y_0 and the value of a and b, we get $drx_0 + dsy_0 = c$

$$d(rx_0 + sy_0) = c$$

Which implies, $d|c$

Conversely assume that, $d|c$

To prove that the linear Diophantine equation has a solution .

If $d|c$ there exist an integer t such that $c = dt$, and the integers x_0 and y_0 satisfying $d = ax_0 + by_0$.

When this relation is multiplied by t, we get, $dt = (ax_0 + by_0)t$

Which implies, $c = a(tx_0) + b(ty_0)$.

Hence the Diophantine equation $ax + by = c$ has $x = tx_0$ and $y = ty_0$ as a particular solution.

If x_0 and y_0 is any particular solution of $ax + by = c$, then $ax_0 + by_0 = c \dots\dots\dots\dots (1)$

If x' and y' are another solution,

then $ax' + by' = c \dots\dots (2)$

From (1) & (2) We have $ax_0 + by_0 = ax' + by'$

Which implies, $a(x' - x_0) = b(y_0 - y')$

Then by corollary of theorem 2.4, there exists relatively prime integers r and s such that $a|d = r$ and $b|d = s$.

Which implies, $a = dr$ and $b = ds$

Substitute the value of a and b, we get

$dr(x' - x_0) = ds(y_0 - y')$

Cancelling the common factor d we write

$r(x' - x_0) = s(y_0 - y')$

Which implies, $s|\, r(x' - x_0)$, with $gcd(r, s) = 1$

By Euclidean lemma, $s|(x' - x_0)$

Which implies, $x' - x_0 = st$, for some integer t

$$\Rightarrow x' = st + x_0$$

$$\Rightarrow x' = x_0 + \left(\frac{b}{d}\right)t$$

Now, $r(x' - x_0) = s(y_0 - y')$

Which implies, $r|s(y_0 - y')$ with $gcd(r, s) = 1$

By Euclid's lemma $r|(y_0 - y')$

$$\Rightarrow y_0 - y' = rt, \text{ for some integer } t$$

$$\Rightarrow y' = y_0 - rt$$

$$\Rightarrow y' = yo - (\tfrac{a}{d})\, t$$

It is easy to see that this values satisfy the Diophantine equation

$$ax' + by' = a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{d}\right)t\right]$$

$$= ax_0 + \left(\frac{ab}{d}\right)t + byo - \left(\frac{ab}{d}\right)t$$

$$= ax_0 + by_0$$

$$= c$$

Thus, there are an infinite number of solution of the given equation one for each value of t.

Example

Solve the linear Diophantine equation $172x + 20y = 1000$.

Solution

Applying the Euclidean's algorithm to $gcd(172{,}20)$

$$172 = 8.20 + 12$$

$$20 = 1.12 + 8$$

$$12 = 1.8 + 4$$

$$8 = 2.4 + 0$$

Therefore, $gcd(172{,}20) = 4$

Since $4|1000$, the solution is exists for this equation.

To obtain the solution, the integer 4 as a linear combination of 172 and 20

$$
\begin{aligned}
\text{Now, } 4 &= 12 - 1.8 \\
&= 12 - 1(20 - 1.12) \\
&= 12 - 1.20 + 1.12 \\
&= 2.12 - 1.12 \\
&= 2(172 - 8.20) - 1.20 \\
&= 2.172 - 16.20 - 1.20 \\
&= 2.172 - 17.20 \\
&= 172(2) + 20(-17)
\end{aligned}
$$

Multiplying the relation by 250 we get,

$1000 = 250[2.172 + (-17)20]$

Hence, $1000 = 500(172) + (-4250)20$

Here $x_0 = 500\,, y_0 = -4250, a = 172, b = 20$

Now, $x = \ x_0 + \left(\frac{b}{d}\right)t$

$$= 500 + \left(\frac{20}{4}\right)t$$

$$x = 500 + 5t$$

Also, $y = \ y_0 - \left(\frac{a}{d}\right)t$

$$= -4250 - \left(\frac{172}{4}\right)t$$

$y = -4250 - 43t$ for some integer t

A little further effort produce the solution in the positive integer

For this, $x > 0 \Rightarrow 500 + 5t > 0$

$\Rightarrow 5t > -500$

$\Rightarrow t > -100$

Also $y > 0 \Rightarrow -4250 - 43t > 0$

$\Rightarrow -43t > 4250$

$\Rightarrow t < -98.84$

Therefore, $-100 < t < -98.84$

Because t must be an integer we conclude that $t = -99$

When $t = -99$

$x = 500 + 5(-99)$

$= 500 - 495$

Therefore, $x = 5$

Also, $y = -4250 - 43(-99)$

$= -4250 + 4257$

Therefore, $y = 7$

Hence $x = 5, y = 7$

Thus, our Diophantine equation has a unique positive solution $x = 5, y = 7$ corresponding to the value $t = -99$

Example

A customer bought a dozen pieces of fruit , apples and oranges for rupees 132. If an apple cost three cents more than orange and more apples than oranges were purchased, how many pieces of each kind were bought.

Solution

We set up this problem as a Diophantine equation.

Let x be a number of apples and y be the number of oranges purchased.

Let z represent the cost of an orange then the condition of problem lead to, $(z+3)x+zy=132$

or $zx+3x+zy=132$

$3x+z(x+y)=132$

Also, given $x+y=12$

Therefore, $3x+12z=132$

Divided by 3, we get, $x+4z \ =44$

We have $gcd(1,4)=1$ and $1|44$

Therefore the solution to this equation exists.

To obtain the solution, write the integer 1 as a linear combination of 1 and 4.

That is, $1=1\times(-3)+4\times 1$

Multiply the relation by 44 We get, $44=1(-132)+4(44)$

Therefore, $x_0=-132\ ,\ \ y_0=44\ ,\ \ a=1,\ \ b=4$

Now, $x = x_0 + \left(\frac{b}{d}\right)t$,

$$x = -132 + \left(\frac{4}{1}\right)t$$

Therefore, $x = -132 + 4t$

Also, $y = yo - (a\backslash d)t$

$$y = 44 - (1)t$$

$y = 44 - t$ for some t

Here, not all of the choices for t furnish solution to the original problem, only values of t that ensure $12 \geq x > 6$ should be consider.

Suppose $12 \geq x$

Then $12 \geq -132 + 4t$

$$\Rightarrow t \leq \frac{144}{4}$$

Therefore $t \leq 36$

Suppose $x > 6$

Then, $-132 + 4t > 6$

$$\Rightarrow \quad t > \frac{138}{4}$$

Therefore, $t > 34.5$

Which gives, $34.5 < t \leq 36$

Since, t must be an integer, we choose $t = 35$ and $t = 36$

When $t = 35$

$$x = -132 + 4(35)$$

$$\Rightarrow x = -132 + 140$$

Therefore, $x = 8$

Also, $y = 44 - 35$

$\Longrightarrow \quad y = 9$

When $t = 36$

$$x = -132 + 4(36)$$

$$x = -132 + 144$$

Therefore, $x = 12$

Also, $y = 44 - 36$

$$y = 8$$

Thus there are two possible purchases.

When $t = 35;$ 8 apples and 4 oranges were purchased.

When $t = 36;$ 12 apples and no oranges were purchased.

Example

If a cock is worth 5 coins a hen 3 coins and 3 chicks together 1 coin how many cocks , hens and chicks totally 100, can be bought for 100 coins ?

Solution

Let x denote the number of cocks and y denote the number of hen and z denote the number of chicks.

Therefore $5x + 3y + \frac{1}{3}z = 100 \dots\dots\dots\dots (1)$

$$x + y + z = 100 \dots\dots\dots\dots (2)$$

From (2) implies $z = 100 - (x + y) \dots\dots\dots\dots..(3)$

Substitute the value of z in (1)

We get, $5x + 3y + \frac{1}{3}(100 - x - y) = 100$

$$\frac{15x + 9y + 100 - x - y}{3} = 100$$

$$14x + 8y + 100 = 300$$

$$14x + 8y = 200$$

Divided by 2, we get $7x + 4y = 100$

To find $gcd(7,4)$

Now, $7 = 1(4) + 3$

$4 = 1(3) + 1$

$3 = 3(1) + 0$

Therefore, $gcd(7,4) = 1$

Because $1|100$, The solution to this equation exists.

To obtain this, the integer 1 as a linear combination of 7 and 4

That is, $1 = 4 - 1.3$

$= 4 - 1(7 - 1.4)$

$= 4 - 1.7 + 1.4$

$= 2.4 - 1.7$

Therefore, $1 = 4(2) + 7(-1)$

Multiply the relation by 100, we get $100 = 4(200) + 7(-100)$

Therefore, $x_0 = -100,\ y_0 = 200\ , a = 7,\ b = 4$

Now, $x = x_0 + \frac{b}{d}t$

Therefore, $x = -100 + 4t$

Also, $y = \ yo - \left(\frac{a}{d}\right) t$

Therefore, $y = 200 - 7t$

Substituting x and y in (3) we get,

$$z \ = 100 - (-100 + 4t) - (200 - 7t)$$

$$= 100 + 100 - 4t - 200 + 7t$$

$$= 3t \text{ , for some integer } t.$$

A little further effort produces the solutions in the positive integers

Therefore, we have, $x > 0 \Longrightarrow -100 + 4t > 0$

$$\Longrightarrow \ 4t > 100$$

$$\Longrightarrow \quad t > 25$$

Also, $y > 0 \quad \Longrightarrow 200 - 7t > 0$

$$\Longrightarrow -7t < -200$$

$$\Longrightarrow t < 28.57$$

Also, $z > 0 \ \Longrightarrow 3t > 0$

$$\Longrightarrow \ t > 0$$

Therefore, we have, $25 < t < 28.57$. Because t must be an integer we conclude that $t = 26,27,28$.

When $t = 26$

$$x = -100 + 4(26) \ = 4$$

$$y = 200 - 7(26) \ = 18$$

$$z = 3(26) = 78$$

when $t = 27$

$x = -100 + 4(27) \ = 8$

$y = 200 - 7(27) \ = 11$

$z = 3(27) \ = 81$

when $t = 28$

$x = -100 + 4(28) \ = 12$

$y = 200 - 7(28) \ = 4$

$z = 3(28) \ = 84$

When $t = 26$ a customer bought 4 cocks, 18 hens and 78 chicks

When $t = 27$ a customer bought 8 cocks,11 hens and 81 chicks

When $t = 28$ a customer bought 12 cocks, 4 hens and 84 chicks

PROBLEMS 2.4

Problem 1

Which of the following Diophantine equation cannot be solved

a) $6x + 51y = 22$

b) $33x + 14y = 115$

Solution

a) $6x + 51y = 22$

Now, $gcd(6,51) = 3$

And 3 doesn't divides 22

Therefore it cannot be solved

b) $33x + 14y = 115$

Now, $gcd(33,14) = 1$

And 1 doesn't divides 115

Therefore it cannot be solved.

Problem 2

A farmer purchased 100 head of livestock for a total cost of Rs.4000 prices were as follow: calves Rs.120 each; lambs Rs.50 each; piglets Rs.25 each. If the farmer obtained at least one animal of each type how many of each did he buy?

Solution

Let x denote the number of heads calves

Let y denote the number of heads lamb

Let z denote the number of heads piglets

Given, $x + y + z = 100 \ldots\ldots\ldots\ldots\ldots (1)$

$120x + 50y + 25z = 4000 \ldots\ldots\ldots\ldots..(2)$

From (1) we have $z = 100 - (x + y) \ldots\ldots\ldots\ldots(3)$

Substitute the value of z in (2) we get,

$120x + 50y + 25(100 - (x + y)) = 4000$

$120x + 50y + 2500 - 25x - 25y = 4000$

$95x + 25y - 1500 = 0$

$95x + 25y = 1500$

$19x + 25y = 300$

Now, to find gcd (19,5)

We have $19 = 3(5) + 5$

$$5 = 1(4) + 1$$

$$4 = 4(1) + 0$$

Therefore, $gcd(19{,}5) = 1.$

Because $1|100$, The solution to this equation exists

To obtain this , write the integer 1 as a linear combination of 19 and 5

We have, $1 = 5 - 1.4$

$$= 5 - (19 - 3.5)$$

$$= 4.5 - 1.19$$

Therefore, $1 = 19(-1) + 5(4)$

Multiply the relation by 300,

we get, $300 = 19(-300) + 5(1200)$

Here, $x_0 = -300,\ y_0 = 1200,\ a = 19,\ b = 5$

$\therefore x = -300 + 5t\ ;\ y = 1200 - 19t$

Substitute x and y in (3), we get

$$z = 100 - (-300 + 5t) - (1200 - 19t)$$

$$z = 100 + 300 - 5t - 1200 + 19t$$

$z = -800 + 14t,$ for some integer t

A little further effort produces the solutions in the positive integers.

Therefore, $z > 0 \Longrightarrow\ -800 + 14t > 0$

$$\Rightarrow \; 14t > 800$$

$$\Rightarrow \; t > 57.14$$

Also, $x > 0 \quad \Rightarrow \quad -300 + 5t > 0$

$$\Rightarrow \; 5t > 300$$

$$\Rightarrow \; t > 60$$

Also we have, $y > 0 \Rightarrow 1200 - 19t > 0$

$$\Rightarrow \; -19t > -1200$$

$$\Rightarrow \; t < 63.16$$

Therefore, $60 < t < 63.16$

Because t must be an integer use conclude that $t = 61,62,63$

When $t = 61$

$$x = -300 + 5(61) \; = 5$$

$$y = 1200 - 19(61) = 41$$

$$z = -800 + 14(61) = 54$$

When $t = 62$

$$x = -300 + 5(62) \; = 10$$

$$y = 1200 - 19(62) = 22$$

$$z = -800 + 14(62) = 68$$

When $t = 63$

$$x = -300 + 5(63) \; = 15$$

$$y = 1200 - 19(63) = 3$$

$$z = -800 + 14(63) = 82$$

Therefore,

When $t = 61$ a farmer bought 5 head of calves 41 head of lambs and 54 head of piglets.

When $t = 62$ a farmer bought 10 head of calves 22 head of lambs and 68 head of piglets.

When $t = 63$ a farmer bought 15 head of calves 3 head of lambs and 82 head of piglets.

Exercise

1) Determine all solutions in the integers of all the following Diophantine Equation a) $56x + 72y = 40$

   b) $24x + 138y = 18$

2) A certain number of sixes and nines is added to give sum of 126 if the number of sixes and nines is interchanged the new sum is 114. How many of each were there originally?

3) Alcuin of York, 775. One hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels each women 2 bushels and child $1/2$ bushels. How many men, women, child are there?

CHAPTER - III

PRIMES AND THEIR DISTRIBUTION

3.1 The Fundamental Theorem Of Arithmetic

Definition

An integer $p > 1$ is called a prime number are simply a prime, if its positive divisors are only 1 and p. An integer which is not a prime is called composite.

Example

Among the first 10 positive integers 2,3,5,7 are prime numbers and 4,6,8,9,10 are composite numbers.

Note

The integer 2 is the only even prime and 1 is neither prime nor composite.

Theorem 3.1

If p is a prime number and $p|ab$ then $p|a$ or $p|b$

Proof

Given p is a prime number and $p|ab$

If $p|a$ then there is nothing to prove. So let us assume that p does not divides a.

Since, the only positive divisor of p are 1 and p itself.

This implies that, gcd$(p, a) = 1$ or $gcd(p, a) = p$

We take , $gcd(p, a) = 1$

Then by Euclid's lemma we get $p|b$

Corollary 3.2

If p is a prime and $p|a_1, a_2, \ldots a_n$ then $p|a_k$ for some k where $1 \leq k \leq n$

Proof

We proceed this theorem by induction of n

When $n = 1$, the stated conclusion is obviously holds.

When $n = 2$ then $p|a_1, a_2$ then by theorem 3.1 we get $p|a_1$ or $p|a_2$

Suppose as the induction hypothesis that n strictly greater than 2 and that whenever p divides a product of less than n factors, it divides at least one of the factors.

Now, let $p|a_1, a_2, \ldots a_n$ then by theorem 3.1, $P|a_1, a_2, \ldots a_{n-1}$ or $p|a_n$

By the induction hypothesis we have $p|a_k$ for some choice of k with $1 \leq k \leq n$

Therefore in any event, p divides one of the integers $a_1, a_2, \ldots a_n$

Corollary 3.3

If $p, q_1, q_2, \ldots, q_n$ are all primes and $p|q_1 . q_2 \ldots q_n$ then $p = q_k$ for some k, $1 \leq k \leq n$.

Proof

By corollary 3.2, we have $p|q_k$ for some k with $1 \leq k \leq n$ being a prime q_k is not divisible by positive integer, other than 1 or q_k itself.

Hence we conclude that $p = q_k$

Theorem 3.4 ***Fundamental Theorem Of Arithmetic***

Every positive integer $n > 1$ can be expressed as a product of primes, this representation is unique, apart from the order in which the factors occur or every positive integer $n > 1$ can be uniquely expressed as a product of primes.

Proof

Let $n > 1$ be any integer. Then either n is prime or it is composite.

Case $\boldsymbol{i}$

If n is a prime, then there is nothing to prove.

Case $\boldsymbol{ii}$

If n is not a prime, then n is a composite number.

If n is composite, then there exists an integer d satisfying $d|n$ and $1 < d < n$

Among all such integers d, choose p_1 to be the smallest. Then p_1 must be a prime number.

Otherwise p_1 would have a divisor q with $1 < q < p_1$.

But $q|p_1$ and $p_1|n$ imply that $q|n$.Which contradicts to the choice of $p_1$as the smallest positive divisor, not equal to 1, of n.

Therefore we may write $n = p_1 n_1$where p_1 is a prime and $1 < n_1 < n$.

If n_1 be a prime, then we have our representation. Otherwise, the argument is repeated to produce second prime number p_2 such that $n_1 = p_1 n_2$; that is, $n = p_1 p_2 n_2$, $1 < n_2 < n$.

If n_2 is a prime then there is nothing to prove otherwise we write, $n_2 = p_3 n_3$ with p_3 is a prime; that is $n = p_1 p_2 p_3 n_3$, $1 < n_3 < n_2$.

The decreasing sequence $n > n_1 > n_2 > n_3 \dots > 1$ cannot continue in the indefinitely, so that after a finite number of steps n_{k-1} is a prime, call it p_k.

This leads to the prime factorization $n = p_1 p_2 \dots p_k$.

Now to prove the uniqueness:

Let us assume that the integers n can be represented as a product of primes in two ways, say $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, $r \leq s$ where p_i and q_j are all primes written in increasing magnitude so that, $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$.

Since $p_1 | q_1 q_2 \dots q_s$ by corollary 2 of theorem 3.1, we have $p_1 = p_k$ for some k.

But we have, $p_1 \geq q_1$ $\dots\dots\dots\dots$ (1)

Similar reasoning gives $q_1 \geq p_1$ $\dots\dots\dots\dots\dots$ (2)

From (1) & (2) we get, $p_1 = q_1$.

We cancel the common factor and obtain the equality $p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$.

Proceeding like this and we get $p_2 = q_2$. Which implies, $p_3 p_4 \dots p_r = q_3 q_4 \dots q_s$

Since, $r < s$ we get, $1 = q_{r+1}q_{r+2} \dots q_s$

Which is a contradiction , because each $q_j > 1$

Hence $r = s$ therefore, $p_1 = q_1, p_2 = q_2, \dots p_r = q_r$

Hence proved.

Corollary 3.5

Any positive integer $n > 1$ written uniquely in a canonical form $n = p_1^{k_1} p_2^{k_2} \dots . p_r^{k_r}$ where $i = 1,2, \dots, r$ each k_i is a positive integer and p_i is a prime with $p_1 < p_2 <, \dots, < p_r$.

Example

Write the canonical form of the integer 360 is $360 = 2^3 \times 3^2 \times 5$

Theorem 3.6 ***Pythagoras***

The number $\sqrt{2}$ is irrational

Proof

To prove $\sqrt{2}$ is irrational**.**

Suppose to the contrary we assume that $\sqrt{2}$ is a rational number, say $\sqrt{2} = \frac{a}{b}$ with $gcd(a, b) = 1$ and a and b are integers.

Squaring on both sides, we get $(\sqrt{2})^2 = \frac{a^2}{b^2}$

$$\Rightarrow \; 2 = \frac{a^2}{b^2}$$

$$\Rightarrow \; 2b^2 = a^2$$

$$\Rightarrow \; b^2 | \, a^2$$

$$\Rightarrow \; b | a^2 \dots \dots \dots \dots \dots (1)$$

If $b > 1$, then the fundamental theorem of arithmetic, then there exists a prime number p such that $p|b \dots \dots \dots \dots (2)$

From (1) & (2) we get, $p|a^2 \dots \dots \dots ..(3)$ then by theorem 3.1, we get $p|a$

Hence, $\gcd(a, b) \geq p$

We therefore arrive at the contradiction, unless $b = 1$. Therefore, the only possibilities is $b = 1$.

Hence, $\sqrt{2} = \frac{a}{b} \quad \Rightarrow \quad \sqrt{2} = a$

$$\Rightarrow \quad a^2 = 2$$

Which is impossible because no integer can be multiplied by itself to give 2.

Therefore, $\sqrt{2}$ is a irrational number.

Theorem 3.7

Prove that the number $\sqrt{3}$ is irrational.

Proof

To prove $\sqrt{3}$ is irrational.

Suppose to the contrary that $\sqrt{3}$ is a rational number, say $\sqrt{3} = \frac{a}{b}$ with $gcd(a, b) = 1$ and a and b are integers.

Squaring on both sides, we get $(\sqrt{3})^2 = \frac{a^2}{b^2}$

$$\Rightarrow 3 = \frac{a^2}{b^2}$$

$$\Rightarrow 3b^2 = a^2$$

$$\Longrightarrow \;\; b^2 |\, a^2$$

$$\Longrightarrow \;\; b|a^2 \ldots\ldots\ldots\ldots.(1)$$

If $b > 1$, then the fundamental theorem of arithmetic, then there exists a prime number p such that $p|b \ldots\ldots\ldots\ldots(2)$

From (1) & (2) we get, $p|a^2 \ldots\ldots\ldots\ldots\ldots.(3)$

By theorem 3.1, we get $p|a.$ Hence, $gcd(a, b) \geq p$

We therefore arrive at the contradiction, unless $b = 1$ therefore, the only possibilities is $b = 1.$

Hence, $\sqrt{3} = \frac{a}{b} \quad \Longrightarrow \quad \sqrt{3} = a$

$\Longrightarrow \;\; a^2 = 3.$

Which is impossible because no integer can be multiplied by itself to give 3.

Therefore $\sqrt{3}$ is a irrational number.

PROBLEMS 3.1

Problem 1

It has been conjectured that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such primes.

Solution

Given $n^2 - 2$

When $n = 2$ gives $2^2 - 2 = 2$, a prime number

When $n = 3$ gives $3^2 - 2 = 7$, a prime number

When $n = 5$ gives $5^2 - 2 = 23$, a prime number

When $n = 7$ gives $7^2 - 2 = 47$, a prime number

When $n = 9$ gives $9^2 - 2 = 79$, a prime number

Therefore, all are prime n numbers.

Problem 2

Prove that any prime of the form $3n + 1$ is also of the form $6m + 1$

Solution

If $3n + 1$ prime implies that $3n + 1$ is odd

Let $= 3n + 1$, then $p - 1 = 3n$ is even**.**

Therefore n is even and $n = 2m$ for some m

Hence, $p = 3(2m) + 1 = 6m + 1$

That is, $p = 6m + 1$

Problem 3

The only prime of the form $n^3 - 1$ is 7

Solution

We know that $(n^3 - 1) = (n - 1)(n^2 + n + 1)$

For $n^3 - 1$ to be a prime, $n > 1$

If $n = 2, n^3 - 1 = (2 - 1)(7) = 7$

For $n > 2, p = n^3 - 1$ will be a factor of two integers, neither of which is one.

Therefore for $\neq 2$, p cannot be a prime.

Hence 7 is the only prime of the form $n^3 - 1$.

Problem 4

Prove that the only prime p for which $3p + 1$ is a perfect square is $p = 5$

Solution

Let p be a given prime number.

Suppose $3p + 1 = n^2$, for some $n \neq 4$.

Therefore $3p = n^2 - 1 = (n + 1)(n - 1)$

If $n + 1 = p$, then $n - 1 = 3$, implies $n = 4$

Suppose we, assume that $n + 1 \neq p$

Therefore $gcd(n + 1, p) = 1$.

Since, $(n + 1)|3p$, by Euclidean Lemma, we have $n + 1 = 3$

Which implies $n = 2$, therefore $3p + 1 = 4$

That is, $p = 1$

Which is a contradiction

Therefore $n + 1$ must be p and therefore n must be 4

Similar reasoning for $n - 1$

If $-1 = p$, then $n + 1 = 3$, $n = 2$ leading to contradiction of $3p + 1 = 4$, that is $p = 1$

Therefore, $n - 1 \neq p$, then gcd$(n - 1, p) = 1$

Therefore,$(n - 1)|3p$ by Euclidean lemma, we have $n - 1 = 1$ or 3

Therefore $n = 4$

Problem 5

The only prime of the form $n^2 - 4$ is 5

Solution

Let $p = n^2 - 4 = (n + 2)(n - 2)$**.**

Since p is prime , one of the factors must be 1 and the other must be p

Suppose $n + 2 = p$, then $n - 2 = 1$

Therefore, $n = 3$

Which gives $p = 5$

Suppose $+2 = 1$, then $n = -1$ therefore $p = n - 2 = -3$

Which given $n + 2 \neq 1$

Therefore, only possibility is $n = 3$

Hence, $p = 5$.

Problem 6

If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite

Solution

Let $p \geq 5$ is a prime number.

By division algorithm, we have $p = 6k + r$, $0 \leq r < 6$

$r \neq 0$ as $p = 6 = 6k \Longrightarrow 6|p$

$r \neq 2$ as $p = 6k + 2 \Longrightarrow 2|p$

$r \neq 3$ as $p = 6k + 3 \Longrightarrow 3|p$

$r \neq 4$ as $p = 6k + 4 \Longrightarrow 4|p$

Therefore, $p = 6k + 1$ or $p = 6k + 5$

Therefore, $p^2 + 2 = 36k^2 + 12k + 3$ or

$$p^2 + 2 = 36k^2 + 60k + 27$$

In either case, $3|p^2 + 2$, so $p^2 + 2$ is composite.

Problem 7

Prove that any integer of the form $8^n + 1$, when $n \geq 1$, is composite

Solution

We know that, $a^3 + 1 = (a + 1)(a^2 - a + 1)$

Therefore, $(2^n)^3 + 1 = (2^n + 1)(2^{2n} - 2^n + 1)$

$\Rightarrow (2^n + 1)|(2^{3n} + 1)$ and $2^{3n} = 8^n$

Hence $(2^n + 1)|(8^n + 1)$

Therefore, $8^n + 1$ is composite.

Problem 8

If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10

Solution

Suppose $10k$ +(even number) can factor out 2, so not a prime number.

Hence, p is of the form $10k + 1, 10k + 3, 10k + 7, 10k + 9$

If $p = 10k + 1$, $(10k + 1)^2 = 100k^2 + 20k + 1$

Therefore $10|(p^2 - 1)$

If $p = 10k + 3$, $(10k + 3)^2 = 100k^2 + 60k + 9$

Now, $p^2 + 1 = 100k^2 + 60k + 10$

Therefore $10|(p^2 + 1)$

If $= 10k + 7$, $(10k + 7)^2 = 100k^2 + 140k + 49$

Now, $p^2 + 1 = 100k^2 + 140k + 50$

Therefore $10|(p^2 + 1)$

If $p = 10k + 9,\ (10k + 9)^2 = 100k^2 + 180k + 81$

Therefore $10|(p^2 - 1)$.

Which gives, either $p^2 - 1$ or $p^2 + 1$ is divisible by 10

Problem 9

Find the prime factorization of the integers $1234, 10140$ and 36000

Solution

$1234 = 2 \times 617$

$$\begin{aligned}10140 &= 10 \times 1014\\ &= 2 \times 5 \times 2 \times 507\\ &= 2^2 \times 5 \times 3 \times 13^2\\ &= 2^2 \times 3 \times 5 \times 13^2\end{aligned}$$

$$\begin{aligned}36000 &= 36 \times 1000\\ &= 2^2 \times 3^2 \times 10 \times 25 \times 4\\ &= 2^2 \times 3^2 \times 2 \times 5^3 \times 2^2\\ &= 2^5 \times 3^2 \times 5^3\end{aligned}$$

Problem 10

It has been conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways.

For example,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \cdots$$

Express the integer 10 as the difference of two consecutive primes in 15 ways.

Solution

$$10 = 149 - 139$$

$$10 = 191 - 181$$

$$10 = 251 - 241$$

$$10 = 293 - 283$$

$$10 = 347 - 337$$

$$10 = 419 - 409$$

$$10 = 431 - 421$$

$$10 = 557 - 547$$

$$10 = 587 - 577$$

$$10 = 701 - 691$$

$$10 = 719 - 709$$

$$10 = 797 - 787$$

$$10 = 821 - 811$$

$$10 = 839 - 829$$

$$10 = 929 - 919$$

3.2 The Sieve of Eratosthenes:

Suppose that we wish to find all primes not exceeding 100. Consider the sequence of consecutive integers

$2,3,4,5,\ldots,100$. Recognizing that 2 is a prime . We begin by crossing out all even integers from our listing except 2 itself. The first of the remaining integers is 3 which must be a prime. We keep 3, strike out all the higher multiples of 3, so that $9,15,21,\ldots$ are now removed. The smallest integer after 3 that has not yet been deleted is 5 it is also a prime. All proper multiples of 5 being composite numbers. We next remove $10,15,20,\ldots$

After eliminating the proper multiples of 7, the largest prime $< \sqrt{100} = 10$, all composite integers in the sequence $2,3,4,\ldots,100$ have fallen through the sieve. The positive integers that remain $2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,$ $67,71,73,79,83,89,97$ are all of the primes < 100 the following table represent the result of the completed sieve the multiples of 2 are crossed out by $\backslash$, the multiples of 3 are crossed out by $/$, the multiples of 5 are crossed out by $-$, the multiples of 7 are crossed out by '$\sim$'

1	2	3	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~

~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~

~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

Therefore, the prime numbers are 2,3,5,7,11,13,17,19,23,29,31, 37,41,43,47,53,59,61,67,71,73,79,83,89,97

Example

Employing the sieve of Eratosthenes obtain all primes between 100 and 200

Solution

Suppose that we wish to find all primes not exceeding 200.Consider the sequence of constructive integers 101,102,…,199 . Recognizing that 101 is a prime.

101 ~~102~~ 103 ~~104~~ ~~105~~ ~~106~~ 107 ~~108~~ 109 ~~110~~

~~111~~ ~~112~~ 113 ~~114~~ ~~115~~ ~~116~~ ~~117~~ ~~118~~ ~~119~~ ~~120~~

121 ~~122~~ ~~123~~ ~~124~~ ~~125~~ ~~126~~ 127 ~~128~~ ~~129~~ ~~130~~

131 ~~132~~ ~~133~~ ~~134~~ ~~135~~ ~~136~~ 137 ~~138~~ 139 ~~140~~

~~141~~ ~~142~~ 143 ~~144~~ ~~145~~ ~~146~~ ~~147~~ ~~148~~ 149 ~~150~~

151 ~~152~~ ~~153~~ ~~154~~ ~~155~~ ~~156~~ 157 ~~158~~ ~~159~~ ~~160~~

~~161~~ ~~162~~ 163 ~~164~~ ~~165~~ ~~166~~ 167 ~~168~~ 169 ~~170~~

~~171~~ ~~172~~ 173 ~~174~~ ~~175~~ ~~176~~ ~~177~~ ~~178~~ 179 ~~180~~

181 ~~182~~ ~~183~~ ~~184~~ ~~185~~ ~~186~~ 187 ~~188~~ ~~189~~ ~~190~~

191 ~~192~~ 193 ~~194~~ ~~195~~ ~~196~~ 197 ~~198~~ 199 ~~200~~

The prime numbers are ;

101,103,107,109,113,121,127,131,137,139,143,149,151,157,163, 167,169,173,179,181,187,191,193,197,199.

Theorem 3.8 ***Euclid***

There is an infinite number of primes.

Proof

We prove this theorem by contradiction method.

Suppose there is a finite number of primes.

Let $p_1 = 2\,, p_2 = 3\,, p_3 = 5\,, p_4 = 7\,, \ldots$ be the primes in ascending order and suppose that there is a last prime called p_n. Now, consider the positive integer $P = p_1, p_2, \ldots, p_n + 1 \ldots \ldots .(1)$

Suppose $P > 1$ then by fundamental theorem of arithmetic be conclude that P is divisible by some prime p; that is $p|P$.

But $p_1 p_2 p_3 \ldots p_n$ are the only prime numbers. So that p must be equal to one of the $p_1, p_2, \ldots, p_n$.

Combining the divisibility relation we get, $p|p_1, p_2, \ldots, p_n$ with $p|P$

$\Rightarrow\ p|(P - p_1 p_2 p_3 \ldots p_n) = p|1$ [by (1)]

The only possible divisor of 1 is 1 itself. Which is a contradiction since $p > 1$

Therefore, there is an infinite number of primes.

Note

For prime p define $p^{\#}$ to be the product of all primes that are less than or equal to p. Numbers of the form $p^{\#} + 1$ might be termed Euclidean numbers, because they appear in Euclid's scheme for proving the infinitude of primes.

For example, $5^{\#} + 1 = 1 \times 2 \times 3 \times 5 + 1 = 31$

Theorem 3.9

If p_n is the n^{th} prime number then $p_n \leq 2^{2^{n-1}}$

Proof

We prove this theorem by induction on n.

When $n = 1,\ p_1 \leq 2^{2^{1-1}}$

$$\implies\ p_1 \leq 2^{2^0}$$

$$\implies p_1 \leq 2^1$$

Therefore, the result is true.

We assume that , $n > 1$ and that the result is true for all integer up to n , then

$$p_{n+1} \leq p_1, p_2, \dots, p_n + 1$$

$$\leq 2,4,16, \dots, 2^{2^{n-1}} + 1$$

$$\leq 2.\, 2^2.\, 2^4 \dots, 2^{2^{n-1}} + 1$$

$$\leq 2^{1+2+4+\cdots+2^{n-1}} + 1$$

But $1 + 2 + 4 + \cdots + 2^{n-1} = \frac{1(2^n-1)}{2-1} = 2^n - 1$

Hence, we obtain, $p_{n+1} \leq 2^{2^{n-1}} + 1$

But, $1 \leq 2^{2^{n-1}}$ for all n

Therefore, $p_{n+1} \leq 2^{2^n-1} + 2^{2^n-1} = 2 \times 2^{2^n-1}$

$$\leq 2 \times \frac{2^{2^n}}{2}$$

Therefore, $p_{n+1} \leq 2^{2^n}$

Corollary 3.10

For $n \geq 1$ there are at least $n+1$ primes less than 2^{2^n}

Proof

From the theorem, 3.9 we know that $p_1, p_2, \ldots, p_n$ are all less than 2^{2^n}

Hence, there are at least $n+1$ primes less than 2^{2^n}

PROBLEMS 3.2

Problem 1

Modify Euclid's proof that there are infinitely many primes by assuming the existence of a largest prime p and using the integer $N = p! + 1$ to arrive at a contradiction.

Proof

Assume that there are finitely many primes, p_n is the largest.

Consider $N = p_n! + 1$

Therefore, $N = 1.2.3 \ldots p_n + 1$ and N must have a prime divisor p_k , $1 \leq k \leq n$.

Since we assuming only finite number of primes,

We have $p_k | 1.2.3 \ldots p_n$ since p_k is one of the number of $p_n!$

Therefore, $p_k | (N - p_1 . p_2 \ldots p_n)$

Which gives, $p_k | 1$ that is $p_k = 1$

Which is a contradiction.

Therefore, there are infinite number of primes.

Problem 2

Let q_n be the smallest prime that is strictly greater than $P_n = p_1p_2 \dots p_n + 1$. It has been conjectured that the difference $q_n - (p_1p_2 \dots p_n)$ is always a prime. Confirm this for the first five values of n

Solution

Given q_n is the smallest prime such that

$q_n > P_n = p_1p_2 \dots p_n + 1$

We have to show that $q_n - (p_1p_2 \dots p_n)$ is a prime for

$n = 1,2,3,4,5$

Now for q_1, we have $1.2 + 1 = 3$

Therefore, $q_1 = 5$

For q_2, we have, $1.2.3 + 1 = 7$

Therefore, $q_2 = 11$

For q_3, we have, $1.2.3.5 + 1 = 31$

Therefore, $q_3 = 37$

For q_4,we have $1.2.3.5.7 + 1 = 211$

Therefore, $q_4 = 223$

For q_5, $1.2.3.5.7.11 + 1 = 2311$

Therefore, $q_5 = 2333.$

Hence, $q_1 - (p_1) = 5 - 2 = 3$

$q_2 - (p_1p_2) = 11 - 6 = 5$

$q_3 - (p_1p_2p_3) = 37 - 30 = 7$

$$q_4 - (p_1 p_2 p_3 p_4) = 233 - 210 = 13$$

$$q_5 - (p_1 p_2 p_3 p_4 p_5) = 2333 - 2310 = 23$$

Hence the result.

Problem 3

If p_n denotes the n^{th} prime number, put $d_n = p_{n+1} - p_n$. An open question is whether the equation $d_n = d_{n+1}$ has infinitely many solutions. Give five solutions.

Solution

Let $d_n = p_{n+1} - p_n$

Find five solutions to $d_n = d_{n+1}$

Now, $d_1 = p_2 - p_1 = 3 - 2 = 1$

$$d_2 = p_3 - p_2 = 5 - 3 = 2$$

$$d_3 = p_4 - p_3 = 7 - 5 = 2$$

Therefore $d_2 = d_3$

$$d_4 = p_5 - p_4 = 11 - 7 = 4$$

$$d_5 = p_6 - p_5 = 13 - 11 = 2$$

$$d_6 = p_7 - p_6 = 17 - 13 = 4$$

$$d_7 = p_8 - p_7 = 19 - 17 = 2$$

$$d_8 = p_9 - p_8 = 23 - 19 = 4$$

$$d_9 = d_{10} - d_9 = 29 - 23 = 6$$

$$d_{10} = d_{11} - d_{10} = 31 - 29 = 2$$

$$d_{11} = d_{12} - d_{11} = 37 - 31 = 6$$

$$d_{12} = d_{13} - d_{12} = 41 - 37 = 4$$

$d_{13} = d_{14} - d_{13} = 43 - 41 = 2$

$d_{14} = d_{15} - d_{14} = 47 - 43 = 4$

$d_{15} = d_{16} - d_{15} = 53 - 47 = 6$

$d_{16} = d_{17} - d_{16} = 59 - 53 = 6$

Therefore $d_{15} = d_{16}$

$d_{17} = d_{18} - d_{17} = 61 - 59 = 2$

$d_{18} = d_{19} - d_{18} = 67 - 61 = 6$

. . .

. . .

. . .

$d_{36} = d_{37} - d_{36} = 157 - 151 = 6$

$d_{37} = d_{38} - d_{37} = 163 - 157 = 6$

Therefore $d_{36} = d_{37}$

. . .

. . .

. . .

$d_{39} = d_{40} - d_{39} = 173 - 167 = 6$

$d_{40} = d_{41} - d_{40} = 179 - 173 = 6$

Therefore $d_{39} = d_{40}$

. . .

. . .

. . .

$d_{46} = d_{47} - d_{46} = 211 - 199 = 12$

$d_{47} = d_{48} - d_{47} = 223 - 211 = 12$

Therefore, $d_{46} = d_{47}$

Therefore the five solutions are $d_2 = d_3$, $d_{15} = d_{16}$, $d_{36} = d_{37}$, $d_{39} = d_{40}$, $d_{46} = d_{47}$

Problem 4

Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that $n > 1$ is either a prime or the product of two primes.

Solution

Given $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$.

Assume that n is composite, and let $n = p_1.p_2 \dots p_r$ and suppose assume $r \geq 3$.

Since p_i is not among the primes $\leq \sqrt[3]{n}$, we have $p_1 > \sqrt[3]{n}, p_2 > p_1 > \sqrt[3]{n}$ ……

We know that $1 < \sqrt[3]{n} < p_i < \sqrt{n}$.

Therefore, $\sqrt[3]{n} < p_1 < \sqrt{n}$

$\sqrt[3]{n} < p_2 < \sqrt{n}$

$\sqrt[3]{n} < p_3 < \sqrt{n}$.

Therefore, $n = (\sqrt[3]{n})(\sqrt[3]{n})(\sqrt[3]{n}) < p_1.p_2.p_3 = n$

Hence, $n < n$ which is a contradiction therefore $r < 3$.

Which implies $= 1\ or\ r = 2$.

Therefore, $n > 1$ is either a prime or the product of two primes.

Problem 5

Show that any composite three-digit number must have a prime factor less than or equal to 31.

Solution

The largest three-digit number is 999.

Now, $\sqrt{999} = 31.6 \ldots$ and 31 is prime, so 31 is the largest prime factor of 999.

Hence, any composite three-digit number must have a prime factor less than or equal to 31.

Problem 6

Give another proof of the infinitude of primes:

Proof

Suppose we assume there is only finite number of primes $p_1 . p_2 \ldots p_n$.

Let A be the product of any r of these $p_1 . p_2 \ldots p_n$.

So $A = p_{a_1} . p_{a_2} . p_{a_3} \ldots . p_{a_r}$, $a_i \in \{1,2 \ldots n\}$

Consider, $B = p_1 . p_2 \ldots p_n / A$

$$= \frac{p_1 . p_2 \ldots p_n}{p_{a_1} . p_{a_2} . p_{a_3} \ldots . p_{a_r}} = p_{b_1} . p_{b_2} . p_{b_3} \ldots . p_{b_s} \text{ where}$$

$a_i \neq b_j$ ($i.e$ factoring out p_{a_i})

So, $\{p_{a_i}\} \cap \{p_{b_i}\} = \emptyset$ and $\{p_{a_i}\} \cup \{p_{b_i}\} = \{p_1 . p_2 \ldots p_n\}$.

So A and B have no common factors. Then each p_k of $p_1 . p_2 \ldots p_n$ divides either A or B, but not both.

Since $A > 1$, $B > 1$, Then $A + B > 1$. Therefore, $A + B$ must have a prime factor, p and $p \in \{p_1, p_2, \ldots, p_n\}$ because we assume finite primes.

Suppose $p|A$ therefore $px = A + B$ for some x and $py = A$ for some y.

Therefore, $px = py + B$.

Which implies $p(x-y) = B$ so $p|B$ which is a contradiction.

Problem 7

Give another proof of the infinitude of primes by assuming that there are only finitely many primes, say $p_1, p_2, \dots, p_n$ and using the following integer to arrive at a contradiction

$N\ = P_2P_3 \dots P_n + P_1P_3 \dots P_n + \cdot\cdot\cdot\ + P_1P_2 \dots P_{n-1}$.

Proof

Suppose we assume there is only finite number of primes $p_1 . p_2 \cdots p_n$.

Consider $q_k = p_1p_2 \dots p_n$ such that each term $p_i \neq q_k$.

Therefore $q_1 = p_2 . p_3 \dots p_n$

$$q_2 = p_1 . p_3 \dots p_n$$

$$\begin{matrix} . & . & . \\ . & . & . \\ . & . & . \end{matrix}$$

$$q_n = p_1 . p_2 \cdots p_{n-1}$$

Therefore, $p_k \nmid q_k$.

Let $N = q_1 + q_2 + \cdots + q_n = \sum_{i=1}^{n} q_i$ then N must have a prime divisor from $p_1, p_2, \dots, p_n$.

Let $p_k (1 \leq k \leq n)$ be the prime divisor, but since $p_k|N$ and $p_k|q_i,\ i \neq k,$

Then $p_k|(N - \sum_{i=1}^{n} q_i)$.

But $N = \sum_{i=1}^{n} q_i = q_k$.

Therefore, $p_k | q_k$ which is a contradiction.

Problem 8

a) Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$.

b) For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer that is greater than n.

Solution

a) For $n > 2$ we have $2n < n! = 1.2 \dots . n$.

Then by Bertrand's Conjecture, there exist a prime p such that $n < p < 2n$.

Therefore, $n < p < 2n < n!$

b) Since $n!$ even for $n > 1$ which implies $n! + 1$ is odd.

Therefore, 2 will never divide $n! + 1$. so, every prime divisor of $n! + 1$ is odd.

Now, it is remain to show that the odd integer is greater than n.

Suppose we assume that every prime divisor p_i of $n! + 1$ less than or equal to n .

Let $p = n! + 1$.

Since p_i is one of the factor of $n!$ we have $p_i | n!$.

Also $p_i | p$.

Therefore, $p_i | (p - n!)$.

Which implies $p_i|1$.

Which is a contradiction since $p_i > 1$.

Therefore, every prime divisor of $n! + 1$ is an odd integer that is greater than n.

Problem 9

Assuming that p_n is the n^{th} prime number, establish each of the following statements:

a) $p_n > 2n - 1$ for n≥ 5.

b) The sum $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ is never an integer.

Solution

a) For $= 5, p_n = 11 > 2(5) - 1 = 9$.

Assume that the result is true for k.

That is, $p_k > 2k - 1$.

Therefore, $p_k + 2 > (2k - 1) + 2 = 2(k + 1) - 1$.

Since $p_k + 1$ is even, then next possible prime is $p_k + 2$.

Therefore, $p_{k+1} > p_k + 2 > 2(k + 1) - 1$.

So, if the result is true for k then it is true for $k + 1$.

Hence, it is true for all $n \geq 5$.

b) Let $= p_1 p_2 \dots p_n$.

And suppose we assume that

$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} = a$ for some integer a.

Therefore, $\frac{p}{p_1} + \frac{p}{p_2} + \cdots + \frac{p}{p_n} = ap.$

For p_1, $p_1|ap \; and \; p_1|\frac{p}{p_2}, p_1|\frac{p}{p_3} \dots, p_1|\frac{p}{p_n}$

Therefore, $p_1|(ap - \frac{p}{p_2} - \frac{p}{p_3} - \cdots - \frac{p}{p_n})$.

Which implies $p_1|p(a - a + \frac{1}{p_1})$

$\Rightarrow p_1|\frac{p}{p_1}$

$\Rightarrow p_1|p_2 \dots p_n$ which is a contradiction.

Similar reasoning applies for $p_2, p_3, \dots, p_n$.

Therefore, the sum $\frac{p}{p_1} + \frac{p}{p_2} + \cdots + \frac{p}{p_n}$ is never an integer.

Problem 10

For the repunits R_n, verify that If $d|R_n$ and $d|R_m$, then $d|R_{n+m}$

[A repunit is an integer written as a string of $1's$, such as $11, 111,$ or 1111. Each such integer must have the form $\left(\frac{10^n - 1}{9}\right)$. We use the symbol R_n to denote the repunit consisting of n consecutive $1's$.]

Solution

We have $R_n = \frac{10^n - 1}{9}$ and $R_m = \frac{10^m - 1}{9}$

Therefore, $R_{n+m} = \frac{10^{n+m} - 1}{9}$

$$= \frac{10^n 10^m - 1}{9}$$

$$= \frac{10^n 10^m - 10^m + 10^m - 1}{9}$$

$$= \frac{10^m (10^n - 1) + 10^m - 1}{9}$$

$$= 10^m R_n + R_m$$

Since, $d|R_n \Longrightarrow R_n = dr$ for some r

$d|R_m \Longrightarrow R_m = ds$ for some s

Therefore, $R_{m+m} = 10^m R_n + R_m$

$$= 10^m dr + ds$$

$$= d(10^m r + s)$$

Which implies $d|R_{n+m}$.

3.3 The Goldbach Conjecture

A pairs of successive odd integers p and $p + 2$ that are both primes is called twin primes**.** It is an unanswered question whether there are infinitely many pairs of twin primes. Numerical evidence leads us to suspect an affirmative conclusion. Electronic computers have discovered 152892 pairs of twin primes less than 30000000 and 20 pairs between 1012 and $10^{12} + 10000$,

Lemma 3.11

The product of two are more integers of the form $4n + 1$ is of the same form.

Proof

It is sufficient to consider the product of just two integers. Let us take $k = 4n + 1$ & $k^{'} = 4m + 1$

Multiplying these together we obtain $kk^{'} = (4n + 1)(4m + 1)$

$$= 6nm + 4n + 4m + 1$$

$$= 4(4nm + n + m) + 1$$

Which is of the decide form.

Therefore, the product of two or more integer of the form $4n + 1$ is of the same form.

Theorem 3.12

There are an infinite number of primes of the form $4n + 3$

Proof

We prove this theorem by contradiction method.

Suppose there are finite number of primes of the form $4n + 3$ called them $q_1, q_2, \dots, q_s$.

Consider the positive integer $N = 4\ q_1 q_2 \dots q_s$

$$= 4\ (q_1 q_2 \dots q_s - 1) + 3$$

Let $N = r_1 r_2 \dots r_k$ be its prime factorization.

Because N is an odd integer, we have $r_k \neq 2$ for all k

So that each r_k is either of the form $4n + 1$ or $4n + 3$

By the lemma, the product of any number of primes of the form $4n + 1$ is again an integer of the form $4n + 1$.

Therefore all the r_k is not of the form $4n + 1$.

For N we take it is of the form $4n + 3$.

Therefore N must contain atleast one prime factor r_i of the form $4n+3$

But r_i cannot be found among the listing $q_1, q_2, \dots, q_s$ for this could leave to the contradiction that $r_i|1$ since $r_i > 1$.

Therefore, the only possible conclusion is that infinitely many primes of the form $4n+3$

Theorem 3.13 ***Dirchlet***

If a and b are relatively prime positive integer then the arithmetic progression $a, a+b, a+2b,\ a+3b, \dots$ contains infinitely many primes.

Co-Prime and Twin Prime

A positive integer having no common factor are called **co-prime**.

If p is a prime number then $p+2$ is also a prime then they are called **twin prime**.

Example

$(3,5), (5,7), (11,13)$ are twin primes

Siamese Prime

If two adjacent integer then they are called **Siamese prime**.

Example

2 &3 are the only Siamese prime.

Theorem 3.14

If all the $n > 2$ terms of arithmetic progression $p, p + d$, $p + 2d, p + 3d, \dots, p + (n - 1)d$ are prime numbers then the common difference d is divisible by every prime $q < n$.

Proof

Consider the prime number $q < n$.

To prove that, the common difference d is divisible by every prime.

That is, to prove that $q|d$

Suppose that q does not divides d that is $q \nmid d$

We claim that the first q terms of the arithmetic progression $p, p + d, p + 2d, p + 3d, \dots, p + (q - 1)d$ will have different remainders when divided by q.

Otherwise there exists integer j and k with $0 \le j \le k \le q - 1$; that is, $k - j \le q - 1 < q$ such that the numbers $p + jd$ and $p + kd$ yield the same remainder upon divided by q.

$\Rightarrow \quad q|(p + jd) \text{ and } \ q|(p + kd)$

$\Rightarrow \quad q|[p + kd - (p + jd)\,]$

$\Rightarrow \quad q|(p + kd - p - jd)$

$\Rightarrow \quad q|(k - j)d$

Which implies, q divides their difference $(k - j)d$

But $gcd(q, d) = 1$.

Then by Euclid’s lemma, we have $q|(k - j)$

Which implies, $k-j>q$

Which is contradiction to the inequality

$k-j \leq q-1<q$ was obtained above.

Hence $p, p+d,\ p+2d, p+3d, \ldots, p+(q-1)d$ will have different remainders when divided by q.

Because the q different remainders produced from $p, p+d, p+2d, p+3d, \ldots, p+(q-1)d$ are drawn from the q integers $0,1,2, \ldots, q-1$, one of these remainder must be zero.

This means that $q|(p+td)$ for some t, satisfying $0 \leq t \leq q-1$.

Because of the inequality $q<n \leq p \leq p+td$, we conclude that $p+td$ is a composite number.

Which is a contradiction.

Hence $q|d$

PROBLEMS 3.3

Problem 1

Verify that the integers 1949 &1951 are twin prime

Solution

If p is a prime number their $p+2$ is also a prime number then they are called twin prime.

Therefore, 1949 is prime and also 1951 is a prime.

Hence, 1949 &1951 are twin prime

Problem 2

Find all pairs of primes such that $p - q = 3$

Solution

Given, $p - q = 3$

$\Longrightarrow p = q + 3$

If q is odd, p is even and > 3 .

But there is no even prime number, $p > 3$.

Therefore q is even and $q = 2$

$\Longrightarrow p = 2 + 3 = 5$.

Therefore, $q = 2$ and $p = 5$ is the only pair of prime such that $p - q = 3$

Problem 3

For $n > 3$, show that the integer's $n, n + 2, n + 4$ cannot all be prime.

Solution

By Division Algorithm, n can be expressed as $n = 6q + r$, $0 \leq r \leq 5$.

We have, $r \neq 0,2,4$ since n would be even.

Therefore $r = 1,3,5$

If $r = 1,\ n = 6q + 1,$ so $n + 2 = 6q + 3$

Which is divisible by 3. Therefore, $r \neq 1$

If $r = 3, n = 6q + 3$.

Which is divisible by 3,So that $r \neq 3$

If $r = 5, n = 6q + 5$, then $n + 4 = 6q + 9$

Which is divisible by 3.

Therefore $r \neq 5$

Therefore, for no value of r can all three members be prime.

Problem 4

Three integers $p, p + 2, p + 6$, which are all prime are called a prime-triplet. Find five sets of prime-triplets.

Solution

When $p = 5$, then $5,7,11$ are prime-triplets

When $p = 11$, then $11,13,17$ are prime-triplets

When $p = 17$, then $17,19,23$ are prime-triplets

When $p = 41$, then $41,43,47$ are prime-triplets

When $p = 101$, then $101,103,107$ are prime-triplets

Problem 5

Find the smallest positive integer n for which the function $f(n) = n^2 + n + 17$ is composite. Do the same for the functions $g(n) = n^2 + 21n + 1$ and $h(n) = 3n^2 + 3n + 23$.

Solution

Given, $f(n) = n^2 + n + 17$

$f(1) = 19$ which is a prime number

$f(2) = 23$ which is a prime number

. . .

. . .

. . .

$f(16) = 289 = 17^2$ is composite.

Also, $g(n) = n^2 + 21n + 1$

$g(1) = 23$ which is a prime number

$g(2) = 47$ which is a prime number

. . .

. . .

. . .

$g(18) = 703 = 19 \times 37$ is composite.

We have, $h(n) = 3n^2 + 3n + 23$

$h(1) = 29$

$h(2) = 41$

. . .

. . .

. . .

$h(22) = 1541 = 23 \times 67$ is composite.

Problem 6

Let p_n denote the n^{th} prime number. For $n \geq 3$, prove that $p^2{}_{n+3} < p_n p_{n+1} p_{n+2}$

Solution

We know that $p_{n+1} < 2p_n$, therefore $p_{n+3} < 2p_{n+2}$

So, $p^2{}_{n+3} < 4p^2{}_{n+2} < 4p_{n+2}(2p_{n+1}) = 8p_{n+2}p_{n+1}$

Since $p_5 = 11$, we have $8p_{n+2}p_{n+1} < p_5 p_{n+2} p_{n+1}$

Therefore $p^2{}_{n+3} < p_n p_{n+1} p_{n+2}$ if $n \geq 5$

For $n = 4$, $p^2{}_7 = 17^2 = 289$

$$< p_4 p_5 p_6$$

$$= 7.11.13 = 1001$$

For $n = 3,\ p^2{}_6 = 13^2 = 169$

$$< p_3 p_4 p_5$$

$$= 5.7.11 = 385$$

For $n = 2,\ p^2{}_5 = 11^2 = 121$

$$< p_2 p_3 p_4$$

$$= 3.5.7 = 105$$

Therefore for $n \geq 3,\ p^2{}_{n+3} < p_n p_{n+1} p_{n+2}$

Problem 7

Let p_n denote the n^{th} prime. For $n > 3$

show that $p_n < p_1 + p_2 + \cdots + p_{n-1}$

Solution

Let p_n denote the n^{th} prime

Here $p_1 = 2, p_2 = 3,$

$p_3 = 5 = 2 + 3 = p_1 + p_2$

And $p_4 = 7 < 2 + 3 + 5 = p_1 + p_2 + p_3$

Therefore assume for $k > 4,\ p_k < p_1 + p_2 + \cdots + p_{k-1}$

Therefore, $2p_k < p_1 + \cdots + p_{k-1} + p_k$

By Bertrand’s Conjecture, there exists p such that, $p_k < p < 2p_k$

But $p_k < p_{k+1} \leq p$

Therefore, $p_{k+1} \leq p < 2p_k < p_1 + \cdots + p_{k-1} + p_k$

Which is true for $k + 1$

Hence $p_n < p_1 + p_2 + \cdots + p_{n-1}$ is true for all $n > 4$.

Problem 8

If p and $p^2 + 8$ are both prime numbers, prove that $p^3 + 4$ is also prime.

Solution

We know that if $p > 3$ is a prime then it is of the form $6k + 1$ or $6k + 5$

Therefore, $p^2 + 8 = (6k + 1)^2 + 8$

$$= 36k^2 + 12k + 9$$

$or \qquad p^2 + 8 = (6k + 5)^2 + 8$

$$= 36k^2 + 60k + 33$$

But, $3|(36k^2 + 12k + 9)$ and $3|(36k^2 + 60k + 33)$

So $p^2 + 8$ is not a prime if $p > 3$.

Therefore we get $p = 3$.

Hence $p^3 + 4 = 31$ is a prime number.

Problem 9

Prove that for every $n \geq 2$ there exists a prime p with $p \leq n < 2p$.

Solution

Case (i) n is odd.

n is odd implies there exist k such that $n = 2k + 1$.

Since $n \geq 2$ we have $k \geq 1$ then by Bertrand's conjecture, there is a prime p such that $k < p \leq 2k$.

Therefore, $p < p + 1 \leq 2k + 1 = n$ so, $p \leq n$.

Also, $2k < 2p$ so $2k + 1 \leq 2p$.

Therefore, $n \leq 2p$. But $n = 2k + 1$ is odd and $2p$ is even.

Hence, $n < 2p$.

Therefore, exists a prime p with $p \leq n < 2p$.

Case (ii) n is even.

n is even implies there exist k such that $n = 2k$

Since $n \geq 2$ we have $k \geq 1$ then by Bertrand's conjecture, there is a prime p such that $k < p \leq 2k$.

Therefore, $p < p + 1 \leq 2k = n$ so, $p \leq n$.

Also, $n = 2k < 2p$

Hence, $n < 2p$.

Therefore, exists a prime p with $p \leq n < 2p$.

Problem 10

Establish that the sequence

$(n + 1)! - 2, (n + 1)! - 3, \ldots, (n + 1)! - (n + 1)$ produces n consecutive composite integers for $n > 2$.

Solution

Since $n > 2$ we have $2 \leq n + 1$ and 2 is in the term of $(n + 1)!$ so $2|[(n + 1)! - 2]$. Therefore $(n + 1)! - 2$ is a composite number.

Similarly 3 is in the term of $(n + 1)!$ so $3|[(n + 1)! - 3]$. Therefore $(n + 1)! - 3$ is a composite number.

Continuing the process at last we get $(n+1)! - (n+1)$ is a composite number.

Therefore, the sequence $(n+1)! - 2, (n+1)! - 3, \dots, (n+1)! - (n+1)$ produces n consecutive composite integers.

CHAPTER - IV

THEORY OF CONGRUENCES

4.1 Basic properties of concurrence:-

Definition

Let n be a fixed positive integer. Two integers a and b are said to be ***congruent modulo n*** symbolized by $a \equiv b(mod\, n)$.If n divides the difference $-b$; that is provided that $a - b = kn$ for some integer k.

Example

Consider $n = 7$ to check that

1) $3 \equiv 24(mod\ 7)$

2) $-31 \equiv 11(mod\ 7)$

3) $-15 \equiv -64(mod\ 7)$

Solution

1) $3 \equiv 24(mod\ 7)$

If $a \equiv b(mod\ n)$ then $a - b = kn$

Therefore $3 - 24 = -21 = 3 \times 7$

$\Longrightarrow \quad 3 \equiv 24(mod\ 7)$

2) $-31 - 11 = -42$

$= -6 \times 7$

$\Longrightarrow -31 \equiv 11(mod\ 7)$

3) $-15 + 64 = 49$

$$= 7 \times 7$$

$$\implies \quad -15 \equiv -64(mod\ 7)$$

Definition

When n does not divides $a-b$; that is $n \nmid a-b)$, we say that $'a'$ is incongruent to b modulus n and in this case we write $a \not\equiv b(mod\ n)$.

Example

$25 \not\equiv 12(mod\ 7)$. Because 7 fails to divide $25-12=13$

Note

Given an integer a.Let q and r be its quotient and remainder upon division by n such that $a = qn + r$, $0 \leq r < n$ then by the definition of congruence $a \equiv r(mod\ n)$

Theorem 4.1

For arbitrary integers a and b, $a \equiv b(mod\ n)$ iff a and b leave the same non-negative remainder when divided by n.

Proof

Assume that $a \equiv b(mod\ n)$

To prove that, a and b leave the same non-negative remainder when divided by n

If $a \equiv b(mod\ n)$, then $n|a-b$

$\implies \quad a-b = kn$ For some integer k

$\implies a = b + kn \quad \ldots\ldots\ldots..(1)$

Upon division by n, b leaves a certain remainder r hence $b = qn + r \ ,0 \leq r < n$

Substitute the value of b in equation (1) we get,

$a \ = qn + r + kn$

$\Longrightarrow \quad a = (q + k)n + r$

Therefore, a and b has the same non-negative remainder r

Conversely, assume that a and b leave the same non-negative remainder when divided by n.

To prove $a \equiv b(mod\ n)$

Suppose we can write, $a = q_1n + r$ and $b = q_2n + r$ with the same remainder, $0 \leq r < n$

Then $a - b = q_1n + r - q_2n - r$

$\Longrightarrow \ a - b = (q_1 - q_2)n$; That is, $n|a - b$

$\Longrightarrow \ a \equiv b(mod\ n)$

Hence the proof.

Theorem 4.2

Let $n > 1$ we fixed and a, b, c, d be arbitrary integers then the following properties hold.

a) $a \equiv a(mod\ n)$

b) If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$

c) If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$ then $a \equiv c(mod\ n)$

d) If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then

$a + c \equiv b + d(mod\ n)$ and $ac \equiv bd(mod\ n)$

e) If $a \equiv b(mod\ n)$ then $a + c \equiv b + c(mod\ n)$ and

$ac \equiv bc(mod\ n)$

f) If $a \equiv b(mod\ n)$ then $a^k \equiv b^k(mod\ n)$ for any positive integer k

Proof

a) For any integer , we have $a - a = 0$

$\Longrightarrow a - a = n.0$

$\Longrightarrow n|a - a$

So that $a \equiv a(mod\ n)$

b) If $a \equiv b(mod\ n)$

$\Longrightarrow p|a - b$

$\Longrightarrow\ a - b = kn$, for some integer k

$\Longrightarrow\ b - a = (-k)n$

$\Longrightarrow\ n|a - b$

$\Longrightarrow b \equiv a(mod\ n)$

c) If $a \equiv b(mod\ n)$ then $n|a - b$

Then there exists an integer k_1 such that $a - b = k_1n\ \ldots\ldots(1)$

If $b \equiv c(mod\ n)$ then $n|b - c$

Then there exists an integer k_2 such that $b - c = k_2n\ldots\ldots(2)$

Adding (1) &(2) we get $a - b + b - c = k_1n\ + k_2n$

$\Longrightarrow a - c = (k_1 + k_2)n$

$\Longrightarrow n|a - c$

$\Longrightarrow a \equiv c(mod\ n)$

d) If $a \equiv b(mod\ n)$ then $n|a-b$

Then there exists an integer h such that $a-b=hn \ldots \ldots.(3)$

If $c \equiv d(mod\ n)$ then $n|c-d$

Then there exists an integer g such that $c-d=gn \ldots \ldots..(4)$

Adding (3) & (4) we get $a-b+c-d=hn+gn$

$$\Longrightarrow (a+c)-(b+d)=(h+g)n$$

$$\Longrightarrow n|(a+c)-(b+d)$$

Therefore, $a+c=b+d(mod\ n)$

From (3) $\Longrightarrow a=b+hn \ldots \ldots \ldots \ldots \ldots (a)$

From (4) $\Longrightarrow c=d+gn \ldots \ldots \ldots \ldots \ldots.(b)$

From (a) & (b) we get, $ac=(b+hn)(d+gn)$

$$=bd+bgn+dhn+hngn$$

$$\Longrightarrow ac-bd=(bg+hd+hgn)n$$

$$\Longrightarrow \quad n|ac-bd$$

Therefore, $ac \equiv bd(mod\ n)$

e) If $a \equiv b(mod\ n)$ then $n|a-b$

Then there exists an integer u such that $a-b=un \ldots \ldots..(5)$

If $c \equiv c(mod\ n)$ then $n|c-c$

Then there exists an integer v such that $c-c=vn \ldots \ldots..(6)$

Adding (5) & (6) we get $a-b+c-c=un+vn$

$$\Longrightarrow (a+c)-(b+c)=(u+v)n$$

$$\Longrightarrow n|(a+c)-(b+c)$$

$$\Longrightarrow \quad a+c \equiv b+c(mod\ n)$$

From (5) $\Longrightarrow \quad a = b + un \ldots\ldots\ldots\ldots (c)$

From (6) $\Longrightarrow \quad c = c + vn \ldots\ldots\ldots\ldots. (d)$

From (c) & (d) we get $ac = (b + un)(c + vn)$

$$= bc + bvn + unc + unvn$$

$\Longrightarrow \; ac - bc = (bv + uc + uvn)n$

$\Longrightarrow n|ac - bc$

Therefore, $ac \equiv bc(mod\, n)$

f) We prove this by induction method for $k = 1$, we have

$a \equiv b(mod\, n)$

Assume the result is true for some k then,

we have $a^k \equiv b^k(mod\, n)$

We prove that, the result is true for some $k + 1$

That is, to prove $a^{k+1} \equiv b^{k+1}(mod\, n)$

If $a \equiv b(mod\, n)$ and $a^k \equiv b^k(mod\, n)$

By Property (d), we have $a. a^k \equiv b. b^k(mod\, n)$

$$\Longrightarrow a^{k+1} \equiv b^{k+1}(mod\, n)$$

Therefore, the result is true for $k + 1$

Hence $a^k \equiv b^k(mod\, n)$ is proved.

Theorem 4.3

If $ca \equiv cb(mod\, n)$ then $a \equiv b(mod\, {}^{n}/_{d})$ where $d = \gcd(c, n)$

Proof

If $ca \equiv cb(mod\, n)$

$\Longrightarrow n|ca - cb$

Then there exists an integer k such that $ca - cb = kn$

$\Longrightarrow \; c(a-b) = kn \ldots\ldots\ldots\ldots..(1)$

Also given, $d = \gcd(c,n)$

$\Longrightarrow \; d|c$ and $d|n$

Then there exists an relatively prime integers r and s such that

$c = dr$ and $n = ds \ldots\ldots\ldots(2)$

Substitute these value in (1) we get, $dr(a-b) = k\,ds$

Canceling the common factor d we get $r(a-b) = ks$

Which implies $s|r(a-b)$

Here, $s|r(a-b)$ with $\gcd(s,r) = 1$

Then by Euclid’s lemma, we have $s|a-b$

$\Longrightarrow a \equiv b(mod\ s)$

From (2) we have, $s = {}^{n}/_{d}$

Therefore $a \equiv b(mod\ {}^{n}/_{d})$

Corollary 4.4

If $ca \equiv cb(mod\ n)$ and $\gcd(c,n) = 1$ then $a \equiv b(mod\ n)$

Corollary 4.5

If $ca = cb\ (mod\ p)$ and $p \nmid c$, where p is a prime number, then $a = b\ (mod\ p)$.

Proof

Given $p \nmid c$ and p a prime imply that $gcd(c,p) = 1$.

Then by Corollary 4.4 we have $a = b\ (mod\ p)$.

Example

1. Consider the congruence $33 \equiv 15(mod\ 9)$

Now, $33 \equiv 15(mod\ 9)$

$\Longrightarrow 3 \times 11 \equiv 3 \times 5(mod\ 9)$

Here, gcd$(3,9) = 3$

Then by theorem we have $11 \equiv 5(mod\ 3)$

PROBLEMS 4.1

Problem 1

Prove each of the following assertions

a) If $a \equiv b\ (mod\ n)$ and $m|n$, then $a \equiv b\ (mod\ m)$

b) If $a \equiv b\ (mod\ n)$ and c>0 , then $ca \equiv cb\ (mod\ cn)$

c) If $a \equiv b\ (mod\ n)$ and the integers a, b, n are all divisible by d>0, then $a/d \equiv b / d\ (mod\ n / d)$

Solution

a) If $a \equiv b\ (mod\ n)$, then prove that $a - b = kn$, for some k

Given, $m|n$ implies that $n = rm$, some r.

Therefore $a - b = krm$, implies that $a \equiv b\ (modm)$

b) If $a \equiv b\ (mod\ n)$ and c>0, then prove that $ca \equiv cb(mod\ cn)$

$a \equiv b\ (mod\ n)$ implies $a - b = kn$, for some k

Therefore, $ca - cb = kcn$ implies that $ca \equiv cb\ (mod\ cn)$

c) If $a \equiv b\ (mod\ n)$, and $d > 0$,then prove that

$a/d \equiv b/d(mod\ n/d)$

Since, $a \equiv b\ (mod\ n)$ implies $a - b = kn$, for some k, By assumption, $a = k_1 d$, then $a/d = k_1$

$b = k_2 d$, then $b/d = k_2$

$n = k_3 d$, then $n/d = k_3$

Therefore, $k_1 d - k_2 d = a - b = kn = k(k_3 d)$

$\Longrightarrow k_1 - k_2 = kk_3$ implies that $a/d - b/d = k(n/d)$

Therefore, $a/d \equiv b/d \pmod{n/d}$

Problem 2

Give an example to show that $a^2 \equiv b^2 \ (mod\ n)$ need not imply that $a \equiv b \ (mod\ n)$

Solution

Take $a = 5$ and $b = 4$

Therefore, $5^2 \equiv 4^2 \ (mod\ 3)$ Since $25 - 16 = 3.3$

But $5 \not\equiv 4 \ (mod\ 3)$

Hence, $a^2 \equiv b^2 \ (mod\ n)$ need not imply that $a \equiv b \ (mod\ n)$.

Problem 3

If $a \equiv b \ (mod\ n)$, Prove that $gcd(a, n) = gcd(b, n)$

Solution

Given $a \equiv b \ (mod\ n)$

To prove $gcd\ (a, n) = gcd(b, n)$

Since $a \equiv b \ (mod\ n)$, we have $a - b = kn$, for some k

Let $d = gcd(a, n)$

Therefore, $a = dr$ and $n = ds$ for some r, s

Which gives $dr - b = kds, \quad b = d(r - ks)$

Therefore $d|b$

Let $d^{'} = gcd(b,n)$

Therefore $d^{'}|n$ and $d^{'}|b$ we get, $d \leq d^{'}$ ……….(1)

By similar reasoning as above, $d^{'}|a$

Therefore $d^{'} \leq d$ ………..(2)

Therefore, from (1) and (2) we get $d^{'} = d$

$\Longrightarrow gcd(a,n) = gcd(b,n)$

Problem 4

Show that 41 divides $2^{20} - 1$

Solution

To prove that, $41|(2^{20} - 1)$

That is, to prove, $2^{20} \equiv 1(mod\ 41)$

We have, $2^{5} \equiv -9(mod\ 41)$

Then by theorem 4.2, (f) we have $(2^{5})^{2} \equiv (-9)^{2}(mod\ 41)$

$\Longrightarrow 2^{10} \equiv 81(mod\ 41)$

$\Longrightarrow 2^{10} \equiv -1(mod\ 41)$ $\quad$ $[\because 81 \equiv -1(mod\ 41)]$

Again by theorem 4.2, (f) we get $(2^{10})^{2} \equiv (-1)^{2}(mod\ 41)$

$2^{20} \equiv 1(mod\ 41)$

Therefore $41|(2^{20} - 1)$

Hence 41 divides $2^{20} - 1$

Problem 5

Find the remainder 2^{50} and 41^{65} are divided by 7

Solution

We have, $2^5 \equiv 4(mod\ 7)$

Then by theorem 4.2, (f) we get, $(2^5)^2 \equiv (4)^2(mod\ 7)$

$$\Rightarrow 2^{50} \equiv 32(mod\ 7)$$

$$\Rightarrow 2^{50} \equiv 4(mod\ 7)$$

Therefore we get the remainder 4 when 2^{50} divided by 7

Now, $41 \equiv 6(mod\ 7)$

$\Rightarrow \quad 41 \equiv -1(mod\ 7)$

$\Rightarrow \quad (41)^5 \equiv (-1)^5(mod\ 7)$

$\Rightarrow \quad (41)^5 \equiv -1(mod\ 7)$

$\Rightarrow (41^5)^{13} \equiv (-1)^{13}(mod\ 7)$

$\Rightarrow \quad 41^{65} \equiv -1(mod\ 7)$

$\Rightarrow \quad 41^{65} \equiv 6(mod\ 7)$

Therefore, we get the remainder 6 when 41^{65}divided by 7

Problem 6

Use the theory of congruent to verify that

$i)$ $89|(2^{44} - 1)$ $ii)$ $97|2^{48} - 1$

Solution

$i)$ To prove that, $89|(2^{44} - 1)$

We have, $2^{11} \equiv 1(mod\ 89)$

The theorem 4.2, (f) we get, $(2^{11})^4 \equiv 1^4(mod\ 89)$

$$\Rightarrow \quad 2^{44} \equiv 1(mod\ 89)$$

$$\Rightarrow 89|(2^{44} - 1)$$

ii) To prove that $97|2^{48}-1$

We have, $2^8 \equiv 35(mod\ 97)$

By Theorem 4.2, (f) we get, $(2^8)^6 \equiv (35)^6(mod\ 97)$

$$\Longrightarrow\ \ 2^{48} \equiv 1838265625(mod\ 97)$$

$$\Longrightarrow\ \ 2^{48} \equiv 1(mod\ 97)$$

$$\Longrightarrow 97|2^{48}-1$$

Problem 7

For $n \geq 1$, Use congruence theory to establish each of the following divisibility statements:

a) $13|(3^{n+2}+4^{2n+1})$

b) $27|(2^{5n+1}+5^{n+2})$

c) $43|(6^{n+2}+7^{2n+1})$

Solution

a) We know that $3 \equiv 16\ (mod\ 13)$

Then $3 \equiv 4^2\ (mod\ 13)$

Therefore $3^n \equiv 4^{2n}\ (mod\ 13)$

$\Longrightarrow 3^n.9 \equiv 4^{2n}.9\ (mod\ 13)$

$\Longrightarrow 3^{n+2} \equiv 4^{2n}.9\ (mod\ 13)$

Therefore, $3^{n+2}+4^{2n+1} \equiv 4^{2n}.9+4^{2n+1}\ (mod\ 13)$

$$\equiv 4^{2n}(9+4)\ (mod\ 13)$$

$$\equiv 4^{2n}(13)(mod\ 13)$$

$$\equiv 0\ \ (mod\ 13)$$

Therefore, $13|(3^{n+2}+4^{2n+1})$

b) We know that $32 \equiv 5\ (mod\ 27)$

Therefore, $2^5 \equiv 5\ (mod\ 27)$

$\Longrightarrow \quad 2^{5n} \equiv 5^n\ (mod\ 27)$

$\Longrightarrow 2^{5n}.2 \equiv 5^n.2\ (mod\ 27)$

Therefore, $2^{5n+1} + 5^{n+2} \equiv 5^n.2 + 5^{n+2}\ (mod\ 27)$

$$\equiv 5^n(2+25)(mod\ 27)$$

$$\equiv 5^n.27\ (mod\ 27)$$

$$\equiv 0\ (mod\ 27)$$

Therefore, $27|(2^{5n+1} + 5^{n+2})$

c) We have $6 \equiv 49\ (mod\ 43)$

Then, $6 \equiv 7^2\ (mod\ 43)$

Therefore, $6^n \equiv 7^{2n}\ (mod\ 43)$

$\Longrightarrow \quad 6^n.36 \equiv 7^{2n}.36\ (mod\ 43)$

Now, $6^{n+2} + 7^{2n+1} \equiv 7^{2n}.36 + 7^{2n+1}\ (mod\ 43)$

$$\equiv 7^{2n}(36+7)\ (mod\ 43)$$

$$\equiv 0$$

Therefore, $43|(6^{n+2} + 7^{2n+1})$

Problem 8

What is the remainder when the following sum is divided by 4?

$1^5 + 2^5 + 3^5 + \cdots \ldots \ldots \ldots + 99^5 + 100^5$

Solution

Since $1^5 \equiv 1\ (mod\ 4)$ and since $1 \equiv 5 \equiv 9 \ldots (mod\ 4)$

$32 = 2^5 \equiv 0\ (mod\ 4)$ and $2 \equiv 6 \equiv 10 \ldots (mod\ 4)$

$243 = 3^5 \equiv 3\ (mod\ 4)$ and $3 \equiv 7 \equiv 11 \ldots (mod\ 4)$

$4^5 \equiv\ 0\ (mod\ 4)$ and $4 \equiv 8 \equiv 12 \ldots (mod\ 4)$

Each block of 4 numbers will have same remainder sum.

Since $1^5 + 2^5 + 3^5 + 4^5 \equiv\ 1 + 0 + 3 + 0 \equiv 4 \equiv 0\ (mod\ 4)$

Then the 25 blocks will all have remainder 0.

Therefore entire remainder is 0.

Problem 9

Prove that, if a is an odd integer, then $a^2 \equiv\ 1\ (mod\ 8)$

Solution

Let a be an odd integer.

By division algorithm, a odd means $a = 4k + 1$ or

$a = 4k + 3$ for some k

Therefore $a^2 = 16k^2 + 8k + 1$ or $a^2 =\ 16k^2 + 24k + 9$

Therefore $a^2 - 1 =\ 8(2k^2 + k)$ or $a^2 - 1 = 8(2k^2 + 3k + 1)$

Which gives, $a^2 \equiv\ 1\ (mod\ 8)$

Problem 10

Give an example to show that $a^k\ \equiv\ b^k\ (mod\ n)$ and

$k \equiv j\ (mod\ n)$ need not imply that $a^j\ \equiv b^j\,(mod\ n)$

Solution

We have $2^2 \equiv 3^2\ (mod\ 5)$ since $4 \equiv 9(mod\ \ 5)$

Also, $2 \equiv 7(mod\ 5)$

But $2^7 \not\equiv 3^7(mod\ 5)$. Because, $2^7 = 128$ and $3^7 = 2187$

Also, $2187 - 128 = 2059$ and 5 does not divides 2059.

4.2 Binary And Decimal Representation Of Integers

Theorem 4.6 ***Special Divisibility Test***

Given an integer > 1 , any positive integer N can be written uniquely interms of power of b as $N = a_m b^m + a_{m-1}\, b^{m-1} + a_{m-2} b^{m-2} + \cdots + a_1 b + a_0$ where the coefficient a_k can on the b different values $0,1,2, \dots , b-1$

Proof

Given, b and N are any two integers.

Then by division algorithm, There exists two integers q_1 and a_0 such that $N = q_1 b + a_0$, $0 \le a_0 < b \dots \dots \dots . (1)$

If $q_1 \ge b$ we can divide one more time with b and obtaining $q_1 = q_2 b + a_1$, $0 \le a_1 < b \dots \dots \dots \dots . (2)$

Now, substitute the value of q_1 in (1) we get,

$N = (q_3 b + a_1) b^2 + a_1 b + a_0$

$\Longrightarrow N = q_3 b^3 + a_1 b^2 + a_1 b + a_0$

Because $N > q_1 > q_2 > \cdots \ge 0$ is a strictly decreasing sequence of integer, this process stop at some stage, say at the $(m-1)$ stage, where $q_{m-1} = q_m b + a_{m-1}$, $0 \le a_{m-1} < b$ and $0 \le q_m < b$

Setting $a_m = q_m$ we get the representation

$N = a_m b^m + a_{m-1}\, b^{m-1} + a_{m-2} b^{m-2} + \cdots + a_1 b + a_0$

Now to prove the uniqueness :

Let us suppose that N has two distinct representation say,

$N = a_m b^m + a_{m-1}\, b^{m-1} + a_{m-2} b^{m-2} + \cdots + a_1 b + a_0$,

$0 \le a_i < b \,\ldots\ldots..(A)$

and $= c_m b^m + c_{m-1}\, b^{m-1} + c_{m-2} b^{m-2} + \cdots + c_1 b + c_0$,

$0 \le c_i < b \,\ldots\ldots\ldots.(B)$

Subtracting (A) from (B) we get,

$$0 = (a_m - c_m)b^m + (a_{m-1} - c_{m-1})b^{m-1} + \cdots + (a_1 - c_1)b + (a_0 - c_0) \;- (C)$$

Therefore, $(c) \Longrightarrow 0 = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0$

Where, $d_i = a_i - c_i$ for $i = 0,1, \ldots, m$

Since the two representation for N are assume to be different, we must have $d_i \neq 0$ for some value of i.

Take k be the smallest subscript for which $d_k \neq 0$ then,

$0 = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_{k+1} b^{k+1} + d_k b^k$

$\Longrightarrow d_k b^k = -(d_m b^m + d_{m-1} b^{m-1} + \cdots + d_{k+1} b^{k+1})$

Now, dividing by b^k we get,

$$d_k = \frac{-(d_m b^m + d_{m-1} b^{m-1} + \cdots + d_{k+1} b^{k+1})}{b^k}$$

$$= -(d_m b^{m-k} + d_{m-1} b^{m-k-1} + \cdots + d_{k+1} b^{k+1-k})$$

$$= \frac{-b(d_m b^{m-k} + d_{m-1} b^{m-k-1} + \cdots + d_{k+1} b)}{b}$$

$$= -b(d_m b^{m-k-1} + d_{m-1} b^{m-k-2} + \cdots + d_{k+1})$$

$\Longrightarrow \quad b | d_k$

$\Longrightarrow \; d_k > b \,\ldots\ldots\ldots\ldots(3)$

Now the inequalities, $0 \leq a_k < b$ and $0 \leq c_k < b$

$\Rightarrow \ -b < a_k - c_k < b$

$\Rightarrow \qquad |a_k - c_k| < b$

$\Rightarrow \qquad\qquad |d_k| < b$

$\Rightarrow \qquad\qquad d_k < b$

Which is a contradiction to (3)

Therefore, $d_k = 0$

Hence, N can be uniquely expressed as,

$$N = a_m b^m + a_{m-1}\, b^{m-1} + a_{m-2} b^{m-2} + \cdots + a_1 b + a_0$$

Theorem 4.7

Let $p(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficient c_k. If $\equiv b(mod\ n)$.

Then $p(a) = p(b)(mod\ n)$

Proof

Given , $p(x) = \sum_{k=0}^{m} c_k x^k$

$$= c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$$

Therefore, $p(a) = c_0 + c_1 a + c_2 a^2 + \cdots + c_m a^m$

$$= \sum_{k=0}^{m} c_k a^k$$

and $p(b) = c_0 + c_1 b + c_2 b^2 + \cdots + c_m b^m$

$$= \sum_{k=0}^{m} c_k b^k$$

Also given, $a \equiv b(mod\ n)$ then by part (f) of theorem 4.2 we get, $a^k \equiv b^k(mod\ n)$ for $k = 0,1,\dots,m$

Therefore, $c_k a^k \equiv c_k b^k(mod\ n)$ for $k = 0,1,\dots,m$

Adding these $m + 1$ congruence we get,

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_m a^m$$

$$= c_0(mod\ n) + c_1 b(mod\ n) + c_2 b^2(mod\ n) + \cdots + c_m b^m(mod\ n)$$

That is $\sum_{k=0}^{m} c_k a^k = \sum_{k=0}^{m} c_k b^k\ (mod\ n)$

Therefore, $p(a) \equiv p(b)(mod\ n)$

Note

If $p(x)$ is a polynomial with integral coefficient, we say that a is a solution of $p(x) \equiv 0(mod\ n)$ if $p(a) = 0(mod\ n)$

Corollary 4.8

If a is a solution of $p(x) \equiv 0(mod\ n)$ and $\equiv b(mod\ n)$ .Then b is also a solution of $p(x) \equiv 0(mod\ n)$.

Proof

Given, a is a solution of $p(x) \equiv 0(mod\ n)$

Therefore, $p(a) \equiv 0(mod\ n)$

Also given, $a \equiv b(mod\ n)$

By theorem 4.4 we get, $p(a) \equiv p(b)(mod\ n)$

$$\Longrightarrow p(b) \equiv p(a)(mod\ n)$$

Then we have, $p(b) \equiv 0(mod\ n)$ $[\because p(a) \equiv 0(mod\ n)]$

Therefore, b is also a solution of $p(x) \equiv 0(mod\ n)$

Example

Calculate $5^{110}(mod\ 131)$

Solution

First note that the exponent 110 can be expressed in binary form

$110 = (1101110)_2 = 64 + 32 + 8 + 4 + 2$

Thus, we obtain the powers $5^{2^j}(mod\ 131)$ for $0 \leq j \leq 6$ by repeatedly squaring while at each stage reducing each result modulo 131

We know that $5^2 \equiv 25(mod\ 131)$

Then, $5^4 \equiv (25)^2(mod\ 131)$

$\Longrightarrow 5^4 \equiv 625(mod\ 131)$

$\Longrightarrow 5^4 \equiv 101(mod\ 131)$

Therefore, $5^4 \equiv -30(mod\ 131)$

Now, $5^8 \equiv (-30)^2(mod\ 131)$

$\Longrightarrow 5^8 \equiv 900(mod\ 131)$

Therefore, $5^8 \equiv 114(mod\ 131)$

We have, $5^8 \equiv -17(mod\ 131)$

$\Longrightarrow (5^8)^2 \equiv (-17)^2(mod\ 131)$

$\Longrightarrow 5^{16} \equiv 289(mod\ 131)$

Therefore, $5^{16} \equiv 27(mod\ 131)$

Now, $(5^{16})^2 \equiv (27)^2(mod\ 131)$

$\Longrightarrow 5^{32} \equiv 729(mod\ 131)$

Therefore, $5^{32} \equiv 74(mod\ 131)$

We have, $5^{32} \equiv -57(mod\ 131)$

$\Longrightarrow (5^{32})^2 \equiv (-57)^2(mod\ 131)$

$\Longrightarrow \quad 5^{64} \equiv 3249(mod\ 131)$

Therefore, $5^{64} \equiv 105(mod\ 131)$

Now, $5^{110} = 5^{64+32+8+4+2}$

$= 5^{64}.5^{32}.5^{8}.5^{4}.5^{2}$

$5^{110} = 5^{64}.5^{32}.5^{8}.5^{4}.5^{2}(mod\ 131)$

$\equiv 105 \times 74 \times 114 \times 101 \times 25(mod\ 131)$

$5^{110} \equiv 2236594500(mod\ 131)$

$5^{110} \equiv 60(mod\ 131)$

Theorem 4.9

Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer $n, 0 \le a_k < 10$ and let $S = a_0 + a_1 + \cdots + a_m$. Then $9|N$ if and only if $9|S$

Proof

Consider $p(x) = \sum_{k=0}^{m} a_k x^k$ be the polynomial with integral coefficient.

That is $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$

We know that, $10 \equiv 1(mod\ 9)$

Then by theorem 4.4 we get, $p(10) \equiv p(1)(mod\ 9) \ldots\ldots..(1)$

Now, we have,

$p(10) = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 = N$ and

$p(1) = a_m + a_{m-1} + \cdots + a_1 + a_0 = S$

Therefore, (1) $\Longrightarrow N \equiv S(mod\ 9)$ it follows that $N \equiv 0(mod\ 9)$ if and only if $S \equiv 0(mod\ 9)$

$\Longrightarrow 9|N$ if and only if $9|S$

Theorem 4.10

Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$ and let $T = a_0 - a_1 + a_2 - \cdots (-1)^m a_m$ .Then $11|N$ if and only if $11|T$

Proof

Consider $p(x) = \sum_{k=0}^{m} a_k x^k$ be the polynomial with integral coefficient.

That is, $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$

We can observe that, $10 \equiv -1(mod\ 11)$

Then by theorem 4.4 we get, $p(10) \equiv p(-1)(mod\ 11) \ldots \ldots (1)$

Now, $p(10) = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 \ = N$

$p(-1) = a_0 - a_1 + a_2 - \cdots (-1)^m a_m \ = T$

Therefore, (1) $\Longrightarrow N \equiv T(mod\ 11)$

It follows that, $N \equiv 0(mod\ 11)\ iff\ T \equiv 0(mod\ n)$

This implies, $11|N$ if and only if $11|T$

PROBLEMS 4.2

Problem 1

Without performing the divisors determine whether the integer 1,571,724 is divisible by 9 or 11

Solution

Take the integer $N = 1571724$ the sum of the integer

$4 + 2 + 7 + 1 + 7 + 5 + 1 = 27$ is divisible by 9.

By theorem 4.5 9 divides $N = 1571724$

It is also can be divided by 11 for this the alternative sum.

$4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$

Here, 11 is divisible by 11

Therefore, by theorem 4.6 we have, 11 divides $N = 1571724$

Problem 2

Without performing the divisors determine whether

$i)$ $176{,}521{,}221$ $ii)$ $149{,}235{,}678$ are divisible by 9 or 11 .

Solution

$i)$ Take the integer $N = 176521221$

The sum of the integer

$1 + 7 + 6 + 5 + 2 + 1 + 2 + 2 + 1 = 27$ is divisible by 9 then by theorem 4.5 we have 9 divides $N = 176521221$

But, this is not divided by 11

For this, the alternating sum is

$1 - 7 + 6 - 5 + 2 - 1 + 2 - 2 + 1 = -3$

Here, -3 is not divisible by 11

$ii)$ Now take the integer $N = 49235678$

The sum of the integer is,

$8 + 7 + 6 + 5 + 3 + 2 + 9 + 4 + 1 = 45$ is divisible by 9

By theorem 4.5 we get, 9 divides N

But, this is not divided by 11

For this, the alternating sum is

$8-7+6-5+3-2+9-4+1=9$

Here, 9 is not divisible by 11

4.3 Linear Congruence and Chinese Remainder Theorem

Definition

An equation of the form $ax \equiv b(mod\, n)$ is called linear congruence. If x_0 is any solution of the linear congruence when it can be written as $ax_0 \equiv b(mod\, n) \Longrightarrow n|ax_0 - b$

$$\Longrightarrow ax_0 - b = kn\,,\ k \in Z$$

Note

The linear congruence $ax \equiv b(mod\, n)$ equivalent to the linear Diophantine equation $ax - ny = b$

Theorem 4.11

The linear congruence $ax \equiv b(mod\, n)$ has the solution if and only if $d|b$ where $d = gcd(a, n)$. If $d|b$ then it has d mutually incongruent solutions modulo n

Proof

Assume that the linear congruence $ax \equiv b(mod\, n)$ has a solution.

To prove that, $d|b$ where $d = gcd(a, n)$

If x_0 is a solution of the linear congruence then,

$ax_0 \equiv b(mod\, n)$

$\implies \quad n|ax_0 - b$

$\implies \quad ax_0 - b = kn\,,\ k \in Z \ldots\ldots..(1)$

Also given, $d = gcd(a,n)$

Which implies, $d|a$ and $d|n$

Then there exists an integers r and s such that $a = dr$ and $n = ds$.

Substitute the value of a and n equation (1),

we get (1) $\implies drx_0 - b = k.ds$

$\implies drx_0 - k.ds = b$

$\implies d(rx_0 - ks) = b$

$\implies d|b$

Conversely, assume that $d|b$

To prove that, the linear congruence $ax \equiv b(mod\, n)$ has a solution.

If $d|b$ then there exists an integer t such that $b = dt$, $t \in Z \ldots\ldots\ldots\ldots.(2)$

Then by theorem 2.3, we get $d = \lambda a - \mu n$

[Given integers a and b not both which of zero there exists an integers x and y such that gcd$(a,b) = ax + by$]

Substitute the value of d in equation (2) we get,

$(2) \implies b = (\lambda a - \mu n)t$

$$\Rightarrow \mathrm{b} = \mathrm{a\lambda t} - \mathrm{n\mu t}$$

$$\Rightarrow a\lambda t - b = n\mu t$$

$$\Rightarrow \mathrm{n|a\lambda t - b}$$

$$\Rightarrow a\lambda t \equiv b(mod\, n)$$

Therefore, $\lambda\mathrm{t}$ is the solution of the linear congruence $ax \equiv b(mod\, n)$

If x_0 and y_0 is any particular solution, then all other solutions has the form $x = x_0 + \left({}^{n}/_{d}\right)t$; $y = y_0 + \left({}^{a}/_{d}\right)t$ for some choice of t.

Among the various integers satisfying first of these formulas. Consider those that occur when $t = 0,1,2, \dots, d-1$

Therefore, $x = x_0,\ x_0 + \frac{n}{d}\ ,\ x_0 + \frac{2n}{d}\ , \dots ,\ x_0 + \frac{d-1}{d}n$

We claim that, these integers are incongruent modulo n and all other such integers are congruent to some one of them.

Suppose, this is happened that,

$x_0 + \left(\frac{n}{d}\right)t_1 \equiv x_0 + \left(\frac{n}{d}\right)t_2(mod\, n)$ where $0 \leq t_1 < t_2 \leq d-1$

Then we would have, $\left(\frac{n}{d}\right)t_1 \equiv \left(\frac{n}{d}\right)t_2(mod\, n)$

Also we have, $gcd\left(\frac{n}{d}\ , n\ \right) = \ \frac{n}{d}$

The common factor $\frac{n}{d}$ should be cancel we arrive at $t_1 \equiv t_2(mod\, d)$ [∵ If $ca \equiv cb\ (mod\, n)$ then $a \equiv b\left(mod\ {}^{n}/_{d}\ \right)$, where $d = gcd(c, n)$]

$\Longrightarrow\ d|t_1 - t_2$

$\Longrightarrow d|t_2 - t_1$ But this is impossible in view of the inequality

$0 < t_2 - t_1 < d$

Therefore, $x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{d-1}{d}n$ are incongruent modulo n and all other such integers are congruent to some one of them.

It remains to show that any other solution $x_0 + \left(\frac{n}{d}\right)t$ is congruent modulo, to one of the d integer listed above.

By division algorithm t can be written as $t = qd + r$ where $0 \leq r \leq d - 1$

Hence, $x_0 + \left(\frac{n}{d}\right)t = x_0 + \left(\frac{n}{d}\right)(qd + r)$

$$= x_0 + nq + r\left(\frac{n}{d}\right)$$

$$= x_0 + \left(\frac{n}{d}\right)r(mod\ n) \text{ with } x_0 + \left(\frac{n}{d}\right)r$$

being one of the solution .

Corollary 4.12

If $\gcd(a, n) = 1$ then the linear congruence $ax \equiv b(mod\ n)$ has a unique solution modulo n.

Theorem 4.13 *Chinese Remainder Theorem*

Let $n_1, n_2, n_3, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $\neq j$. Then the system of linear congruences

$$x \equiv a_1(mod\ n_1)$$

$x \equiv a_2 (mod\, n_2)$

. . .

. . .

. . .

$x \equiv a_r (mod\, n_r)$

has a simultaneous solution which is unique modulo to the integers $n_1, n_2, n_3, \dots, n_r$

Proof

We begin the proof by forming the product $n = n_1 . n_2 . n_3 \dots n_r$ for each $k = 1,2,3, \dots, r$

Let $N_k = \frac{n}{n_k} = \frac{n_1 . n_2 . n_3 \dots n_r}{n_k}$

$$= \frac{n_1 n_2 n_3 \dots n_{k-1} n_{k+1} \dots n_r}{n_k}$$

Therefore, $N_k = n_1 n_2 n_3 \dots n_{k-1} n_{k+1} \dots n_r$ in words N_k is the product of all integers n_i,with the factor n_k omitted.

Given , $\gcd(n_i, n_j) = 1$

Therefore, n_i are relatively prime in pairs. So that $\gcd(N_k, n_k) = 1$

Then by corollary, the linear congruence $N_k x \equiv 1 (mod\, n_k)$ has a unique solution. [If $\gcd(a, n) = 1$ then the linear congruence $ax \equiv b (mod\, n)$ has a unique solution modulo n]

We call the unique solution as x_k

Next our aim is to prove that, the integer $\overline{x} = a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r$ is the simultaneous solution of the given system,

First observe that, $N_i \equiv 0(mod\, n_k)$ for $i \neq k$ since $n_k|N_i$

In this case $\overline{x} = a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r$

$$= a_kN_kx_k(mod\, n_k) \dots \dots (1)$$

But the integer x_k was choosen to satisfy the congruence $N_kx \equiv 1(mod\, n_k)$

This implies, $\overline{x} \equiv a_k.1(mod\, n_k\,)$

$$\Longrightarrow \quad \overline{x} \equiv a_k(mod\, n_k\,)$$

This shows that the solution to the given system of congruence exists.

Next to prove the uniqueness,

Let $x^{'}$ be another integer to the given system of linear congruence.

Then $\overline{x} \equiv a_k \equiv x^{'}(mod\, n_k), k = 1,2, \dots, r$ and so $n_k|(\overline{x} - x^{'})$ for each value of k.

That is $n_1|\overline{x} - x^{'}\,, n_2|\overline{x} - x^{'}\,\,, \dots, n_r|\overline{x} - x^{'}$

Also since, $\gcd(n_i, n_j) = 1$

Then by corollary, we have $n_1n_2 \dots n_r|\overline{x} - x^{'}$

[If ${}^{a}/_{c}$ and ${}^{b}/_{c}$ with $\gcd(a, b) = 1$ then ${}^{ab}/_{c}$]

$$\Longrightarrow \quad \overline{x} \equiv x^{'}(mod\, n_1n_2 \dots n_r)$$

$$\Longrightarrow \quad \overline{x} \equiv x^{'}(mod\, n)$$

Theorem 4.14

The system of linear congruence

$ax + by \equiv r(mod\, n)$

$cx + dy \equiv s(mod\, n)$

has a unique solution modulo n whenever gcd$(ad - bc, n) = 1$.

Proof

Given, $ax + by \equiv r(mod\, n) \dots\dots\dots (1)$

$cx + dy \equiv s(mod\, n) \dots\dots\dots (2)$

Multiply the first congruence by d, we get

$acx + bdy \equiv rd(mod\, n) \dots\dots\dots (3)$

Multiply the second congruence by b we get

$bcx + bdy \equiv sb(mod\, n) \dots\dots\dots (4)$

Now $(3) - (4)$ we get,

$(ad - bc)x = dr - bs(mod\, n) \dots\dots\dots (5)$

Multiply the first congruence by c

$acx + bcy \equiv rc(mod\, n) \dots\dots\dots. (6)$

Multiply the second congruence by a

$acx + ady \equiv as(mod\, n) \dots\dots\dots. (7)$

Now, $(7) - (6)$ we get,

$(ad - bc)y = as - cr(mod\, n) \dots\dots\dots. (8)$

And also given, gcd$(ad - bc, n) = 1$

Therefore, $(ad - bc)z \equiv 1(mod\, n)$ has a unique solution modulo n denote the solution by t

When the congruence (5) is multiply by t we get,

$t(ad - bc)x \equiv (dr - bs)t\ (mod\ n)$

$\Longrightarrow x \equiv (dr - bs)t(mod\ n)$ and when the congruence equation (8) is multiply by t we get, $t(ad - bc)y = (as - cr)t(mod\ n)$

$\Longrightarrow y \equiv (as - cr)t(mod\ n)$

PROBLEMS 4.3

Problem 1

Solve the following linear congruence

a) $25x \ \equiv\ 15\ (mod\ 29)$

b) $5x \quad \equiv\ 2\ (mod\ 26)$

c) $6x \quad \equiv\ 15\ (mod\ 21)$

d) $36x \ \equiv\ 60\ (mod\ 98)$

e) $34x \ \equiv\ 60\ (mod\ 98)$

f) $140x \equiv 133\ (mod\ 301)$

Solution

a**)** Given, $25x \ \equiv\ 15(mod\ 29)\ \ \ldots\ldots\ldots..(1)$

Here, $gcd\ (25{,}29) = 1$

Therefore, solution exists.

We have, $-29x \equiv 29(mod29)\ \ldots\ldots\ldots..(2)$

Adding (1) & (2) we get, $-4x \equiv -14(mod\ 29)$

$\Longrightarrow \quad 2x \equiv\ 7(mod\ 29),$ (since $gcd\ (2{,}29) = 1$)

$\Longrightarrow 30x\ \equiv 105(mod\ 29\ \ldots\ldots\ldots\ldots..(3)$

Adding (2) & (3) we get, $x\ \equiv\ 76(mod\ 29)$

Therefore, $x \equiv 18 \ (mod\ 29)$

b) Given, $5x \equiv 2 \ (mod\ 26)$

Here, gcd(5,26) = 1. Therefore, solution exists.

Now, $5x \equiv 2 \ (mod\ 26) \Longrightarrow 25x \equiv 10(mod\ 26) \ \ldots \ldots (1)$

We have, $-26x \equiv -26(mod 26) \ \ldots \ldots \ldots (2)$

Adding (1) & (2) we get, $25x - 26x \equiv 10 - 26 \ (mod\ 26)$

$$\Longrightarrow -x \equiv -16(mod\ 26)$$

Therefore, $x \equiv 16 \ (mod 26)$

c) $6x \equiv 15 \ (mod\ 21)$

Here, $gcd\ (6,21) = 3\ and\ 3|15$. Therefore, solution exists.

Now, $6x \equiv 15 \ (mod\ 21) \Longrightarrow 2x \equiv 5 \ (mod\ 7) \ldots \ldots \ldots (1)$

$[\because\ divided\ by\ 3]$

We have, $0 \equiv 7(mod 7) \ \ldots \ldots \ldots . (2)$

Adding (1) & (2) we get, $2x \equiv 12 \ (mod\ 7)$,

$\Longrightarrow x \equiv 6 \ (\ mod\ 7)$, since $gcd\ (\ 2,7) = 1$ and divide by 2.

Therefore, $x = 6 + 7t$

Since, gcd$(6,21) = 3$, then there are 3 mutually incongruent solutions by putting $t = 0,1,2$

Therefore, $x = 6,13,20 \ (mod\ 21)$

d) $36x \equiv 8(mod\ 102)$

Here, $gcd\ (36,102) = 6$ and 6 does not divides 8

Therefore, there is no solution.

e) $36x \equiv 60 \ (\ mod\ 98)$

Here, $gcd\ (34{,}98) = 2$ and $2|60$

Therefore, solution exists.

Now, $36x \equiv 60(\,mod\ 98) \Longrightarrow 102x \equiv 180(\,mod\ 98)\ \ldots(1)$

We have, $-98 \equiv -2.98(mod 98)\ \ldots..(2)$

Adding (1) & (2) we get,

$102x - 98x \equiv 180 - 2.98(mod\ 98)$

$\Longrightarrow 4x \equiv -16\ (mod\ 98)$

$\Longrightarrow 2x \equiv -8(mod\ 49)$

$\Longrightarrow x \equiv -4\ (mod\ 49)$

Therefore, $x = -4 + 49t$

Hence, there are two incongruent solutions exists.

For, $t = 0{,}1$ implies that $x \equiv -4\ {,}45\ (mod\ 98)$ or

$x = 45{,}94\ (mod\ 98)$

f) $140x \equiv 133\ (mod\ 301)$

Now, $140 = 2^2.5.7$ and $301 = 7 \times 43$

Therefore, $gcd\ (140, 301) = 7$ and $7|133$

Therefore, there are 7 incongruent solutions exists.

Now, $140x \equiv 133\ (mod\ 301)$

$\Longrightarrow 20x \equiv 19\ (mod\ 43)$

$\Longrightarrow 40x \equiv 38\ (mod\ 43)\ \ldots\ldots..(1)$

We have, $43x \equiv 43(mod\ 43)\ \ldots\ldots\ldots(2)$

Subtracting (1) from (2) we get,

$43x - 40x \equiv 43 - 38\ (mod\ 43)$

$\Longrightarrow\ 3x\ \equiv\ 5\ (mod\ 43)$

$\Longrightarrow 42x \equiv\ 70\ (\ mod\ 43)\ \dots\dots(3)$ (multiply by 14)

Subtracting (3) from (1) we get,

$43x - 42x \equiv\ 86 - 70\ (mod\ 43)$

$\Longrightarrow x \equiv\ 16\ (mod\ 43)$

Therefore, $x =\ 16 + 43t$.

We have to get solutions putting $t = 0, 1,2,3,4,5,6.$

Which gives, $x \equiv 16,59,102,145,188,231,274\ (mod\ 301).$

Problem 2

Solve the linear congruence $18x \equiv 30(mod\ 42)$

Solution

Given $18x \equiv 30(mod\ 42)$

Here $a = 18\ , b = 30\ , n = 42$

Now, $\gcd(a, n) = \gcd(18,42) = 6$

Then by theorem 4.11, the linear congruence has exactly 6 solutions.

$18x \equiv 30(mod\ 42)\ \dots\dots\dots..(1)$

Also, $42 \equiv 0(mod\ 42)$

$\Longrightarrow 0 \equiv 42(mod\ 42)\ \dots\dots..(2)$

$[\ \because a \equiv b(mod\ n), b \equiv a(mod\ n)\ ]$

Therefore, $(1) + (2) \Longrightarrow 18x \equiv 72(mod\ 42)$

$\Longrightarrow\quad x \equiv 4(mod\ 42)$

Therefore, one solution is found to be $x_0 = 4$ and all other solution is of the form $x_0 + \left(\frac{n}{d}\right)t$, where $t = 0,1,2,3,4,5$

When $t = 0$,

$$x = x_0 + \left(\frac{n}{d}\right)t = 4 + \left(\frac{42}{6}\right) \times 0 = 4$$

When $t = 1$,

$$x = x_0 + \left(\frac{n}{d}\right)t = 4 + \left(\frac{42}{6}\right) \times 1 = 11$$

When $t = 2$,

$$x = x_0 + \left(\frac{n}{d}\right)t = 4 + \left(\frac{42}{6}\right) \times 2 = 18$$

When $t = 3$,

$$x = x_0 + \left(\frac{n}{d}\right)t = 4 + \left(\frac{42}{6}\right) \times 3 = 25$$

When $t = 4$,

$$x = x_0 + \left(\frac{n}{d}\right)t = 4 + \left(\frac{42}{6}\right) \times 4 = 32$$

When $t = 5$,

$$x = x_0 + \left(\frac{n}{d}\right)t = 4 + \left(\frac{42}{6}\right) \times 5 = 39$$

Therefore the six solutions are $x \equiv 4,11,18,25,32,39(mod\ 42)$

Problem 3

Solve the linear congruence $9x \equiv 21(mod\ 30)$

Solution

Given, $9x \equiv 21(mod\ 30)$

Here $a = 9\,, b = 21\,, n = 30$

Now, $\gcd(a, n) = 3$

Then by theorem 4.11, the linear congruence has exactly 3 solutions.

$9x \equiv 21(mod\ 30) \ldots\ldots\ldots..(1)$

We have, $60 \equiv 0(mod\ 30)$

$\Longrightarrow 0 \equiv 60(mod\ 30) \ldots\ldots\ldots.(2)$

$(1) + (2) \Longrightarrow 9x \equiv 81(mod\ 30)$

$\qquad\qquad \Longrightarrow \ x \equiv 9(mod\ 30)$

Therefore the one solution is found to be $x_0 = 9$ and all other solution is of the form $x_0 + \left(\frac{n}{d}\right)t$, where $t = 0,1,2$

When $t = 0$,

$x = x_0 + \left(\frac{n}{d}\right)t = 9$

When $t = 1$,

$x = x_0 + \left(\frac{n}{d}\right)t = 19$

When $t = 2$,

$x = x_0 + \left(\frac{n}{d}\right)t = 29$

Therefore, the three solution of $x \equiv 9,19,29(mod\ 30)$

Problem 4

Solve the linear congruence $25x \equiv 15(mod\ 29)$

Solution

Given, $25x \equiv 15(mod\ 29)$

Here $a = 25\ , b = 15\ , n = 29$

Now, $\gcd(a, n) = 1$

Then by theorem 4.11,

The linear congruence has exactly one solution.

$25x \equiv 15(mod\ 29) \dots \dots \dots (1)$

We have, $435 \equiv 0(mod\ 29)$

$\Longrightarrow \ \ 0 \equiv 435(mod\ 29) \dots \dots \dots \dots (2)$

$(1) + (2) \ \Longrightarrow 25x \equiv 450(mod\ 29)$

$$x \equiv 18(mod\ 29)$$

Therefore the one solution is found to be $x_0 = 18$ and all other solution is of the form $x_0 + \left(\frac{n}{d}\right) t$, where $t = 0$

When $t = 0$

$x = x_0 + \left(\frac{n}{d}\right) t = 18$

Therefore, the solution is $x \equiv 18(mod\ 29)$

Problem 5

Solve the linear congruence $6x \equiv 15(mod\ 21)$

Solution

Given, $6x \equiv 15(mod\ 21)$

Here $a = 6\ , b = 15\ , n = 21$

Now, $gcd(a, n) = 3$

Then by theorem 4.11, the linear congruence has exactly 3 solutions

$6x \equiv 15(mod\ 21) \dots\dots\dots\dots (1)$

We have, $21 \equiv 0(mod\ 21)$

$\Longrightarrow 0 \equiv 21(mod\ 21) \dots\dots\dots..(2)$

$(1) + (2) \ \Longrightarrow 6x \equiv 36(mod\ 21)$

$$x \equiv 6(mod\ 21)$$

Therefore, the one solution is found to be $x_0 = 6$ and all other solution is of the form $x_0 + \left(\frac{n}{d}\right)t$, where $t = 0,1,2$

When $t = 0$,

$x = x_0 + \left(\frac{n}{d}\right)t = 6$

When $t = 1$,

$x = x_0 + \left(\frac{n}{d}\right)t = 13$

When $t = 2 \ \ x = x_0 + \left(\frac{n}{d}\right)t = 20$

Therefore, the three solution of $x \equiv 6{,}13{,}20(mod\ 21)$

Problem 6

Solve the linear congruence $9x \equiv 21(mod\ 30)$ using Diophantine equation.

Solution

Given, $9x \equiv 21(mod\ 30)$

$\Longrightarrow 30|9x - 21$

$\Longrightarrow 9x - 21 = 30y$

$\Longrightarrow 9x - 30y = 21$

$\Longrightarrow 9x + 30(-y) = 21$

To solve the linear Diophantine equation $9x - 30y = 21$

Using the Euclidean algorithm to find gcd$(9{,}30)$

Now, $30 = (3)9 + 3$

$9 = (3)3 + 0$

Therefore, $gcd(9{,}30) = 3$

Since, $3|21$ a solution to this equation exists.

To obtain this the integer 3 as a linear combination of 9 and 30

That is $3 = 30 - 3.9$

$\Longrightarrow 3 = 30 + 9(-3)$

Multiply the relation by 7, we get $21 = 9(-21) - 30(-7)$

Therefore, $x_0 = -21\,,\ \ y_0 = -7\,,\ \ b = 30\,,\ \ a = 9$

Now, $x = x_0 + \left(\frac{b}{d}\right)t \quad \Longrightarrow x = -21 + \left(\frac{30}{3}\right)t$

$\Longrightarrow x = -21 + 10t\,, t = 0{,}1{,}2$

When $t = 0\,, x = -21$

When $t = 1\,, x = -11$

When $t = 2\,, x = -1$

Therefore, the 3 incongruence solutions are

$x \equiv -21(mod\ 30)\,,\ \ x \equiv -11(mod\ 30)\,, x \equiv -1(mod\ 30)$

$i.e)\ x \equiv 9(mod\ 30), x \equiv 19(mod\ 30), x \equiv 29(mod\ 30)$

Problem 7

Solve the system of congruence

$x \equiv 2(mod\ 3)$

$x \equiv 3(mod\ 5)$

$x \equiv 2(mod\ 7)$

Solution

Given, $x \equiv 2(mod\ 3)$

$x \equiv 3(mod\ 5)$

$x \equiv 2(mod\ 7)$

Here $a_1 = 2\ , a_2 = 3\ , a_3 = 2\ , n_1 = 3\ , n_2 = 5\ , n_3 = 7$

Now, $n = n_1 \times n_2 \times n_3$

$= 3 \times 5 \times 7$

$= 105$

Also, $N_k = \frac{n}{n_k}$

Now, $N_1 = \frac{n}{n_1} = \frac{105}{3} = 35$

$N_2 = \frac{n}{n_2} = \frac{105}{5} = 21$

$N_3 = \frac{n}{n_3} = \frac{105}{7} = 15$

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

And, $gcd(N_1, n_1) = gcd(35,3) = 1$

Therefore, $35x \equiv 1(mod\ 3) \dots \dots (1)$ has a unique solution

[∵ If $\gcd(a,n) = 1$ then the linear congruence $ax \equiv b(mod\ n)$ has a unique solution]

Also we have, $69 \equiv 0(mod\ 3)$

$\Longrightarrow 0 \equiv 69(mod\ 3) \dots .. (2)$

$(1) + (2) \Longrightarrow 35x \equiv 70(mod\ 3)$

$\Longrightarrow \quad x \equiv 2(mod\ 3)$

Therefore, one of the solution is $x_1 = 2$

Now, $\gcd(N_2, n_2) = \gcd(21,5) = 1$

Which implies, $21x \equiv 1(mod\ 5) \dots \dots .. (3)$ has a unique solution.

We have, $20 \equiv 0(mod\ 5)$

$\Longrightarrow \quad 0 \equiv 20(mod\ 5) \dots \dots .. (4)$

$(3) + (4) \Longrightarrow 21x \equiv 21(mod\ 5)$

$x \equiv 1(mod\ 5)$

Therefore, $x_2 = 1$ is a solution.

Now, $\gcd(N_3, n_3) = \gcd(15,7) = 1$

By a theorem we have $15x \equiv 1(mod\ 7) \dots \dots \dots (5)$ has a unique solution.

We have, $14 \equiv 0(mod\ 7)$

$\Longrightarrow 0 \equiv 14(mod\ 7) \dots \dots .. (6)$

$(5) + (6) \Longrightarrow 15x \equiv 15(mod\ 7)$

$x \equiv 1(mod\ 7)$

Therefore, $x_3 = 1$ is a solution.

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

$= 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$

$= 140 + 63 + 30$

$\overline{x} = 233$

Therefore, $\overline{x} \equiv 233(mod\ 105)$

Hence, $\overline{x} \equiv 23(mod\ 105)$

Problem 8

Consider the system,

$7x + 3y \equiv 10(mod\ 16)$

$2x + 5y \equiv 9(mod\ 16)$

Solution

Given, $7x + 3y \equiv 10(mod\ 16) \dots\dots\dots..(1)$

$2x + 5y \equiv 9(mod\ 16) \dots\dots\dots\dots(2)$

Here $a = 7, b = 3,\ c = 2\ ,\ d = 5\ ,\ n = 16$

$(1) \times 2 \Longrightarrow\ \ 14x + 6y \equiv 20(mod\ 16) \dots\dots\dots.(3)$

$(2) \times 7 \Longrightarrow 14x + 35y \equiv 63(mod\ 16) \dots\dots\dots(4)$

$(3) - (4) \Longrightarrow\ -29y \equiv -43(mod\ 16)$

$29y \equiv 43(mod\ 16) \dots\dots\dots..(5)$

$(1) \times 5 \Longrightarrow 35x + 15y \equiv 50(mod\ 16) \dots\dots\dots..(6)$

$(2) \times 3 \Longrightarrow\ \ 6x + 15y = 27(mod\ 16) \dots\dots\dots..(7)$

$(6) - (7) \Longrightarrow 29x \equiv 23(mod\ 16) \dots\dots\dots..(8)$

Now, $gcd(ad - bc, n) = gcd(35 - 6,16)$

$= gcd(29,16) = 1$

Therefore, the linear congruence has unique solution.

Consider the congruence, $(5) \Longrightarrow 29y \equiv 43(mod\ 16) \dots \dots \dots (9)$

We have, $160 \equiv 0(mod\ 16) \Longrightarrow 0 \equiv 160(mod\ 16) \dots \dots .. (10)$

$(9) + (10) \Longrightarrow 29y \equiv 203(mod\ 16)$

$\Longrightarrow y \equiv 7(mod\ 16)$

Now, $(8) \Longrightarrow 29x \equiv 23(mod\ 16) \dots \dots .. (11)$

We have, $64 \equiv 0(mod\ 16)$

$\Longrightarrow 0 \equiv 64(mod\ 16) \dots \dots . (12)$

$(11) + (12) \Longrightarrow 29x \equiv 87(mod\ 16)$

$x \equiv 3(mod\ 16)$

Therefore, the solutions are $x \equiv 3(mod\ 16), y \equiv 7(mod\ 16)$

Problem 9

Using congruences, solve the Diophantine equation below:

a) $4x + 51y = 9$

Solution

Given, $4x + 51y = 9$

$\Longrightarrow \quad 4x - 9 = -51y$

$\Longrightarrow \quad 51|4x - 9$

$\Longrightarrow \quad 4x \equiv 9(mod 51)$

Here $a = 4\ , b = 9\ , n = 51$

Now, $\gcd(a, n) = 1$

By theorem 4.11, the linear congruence has exactly one solution.

$4x \equiv 9(mod 51) \dots \dots . (1)$

We have, $51 \equiv 0(mod\ 51)$

$\Longrightarrow\ 0 \equiv 51(mod\ 51) \dots\dots\dots.(2)$

$(1) + (2) \Longrightarrow 4x \equiv 60(mod\ 51)$

$\Longrightarrow\ x \equiv 15(mod\ 51)$

Therefore, one solution is found to be $x_0 = 15$ and all other solutions is of the form $x_0 + \left(\frac{n}{d}\right)t,$ where $t = 0$

When $t = 0\,, x = 15 + \frac{51}{1}(0) = 15$

Therefore, the solution is $x \equiv 15(mod\ 51)$

Given Diophantine equation is $4x + 51y = 9$

At (x_0, y_0), we have $4x_0 + 51y_0 = 9$

$$\Longrightarrow 4 \times 15 + 51y_0 = 9$$

$$\Longrightarrow \qquad 51y_0 = 9 - 60$$

$$\Longrightarrow \qquad y_0 = \frac{-51}{51}$$

$$\Longrightarrow \qquad y_0 = -1$$

Therefore, the solution to Diophantine equation is $x = 15$ & $y = -1$

Problem 10

Using congruences, solve the Diophantine equation below:

$12x + 25y = 331$

Solution

Given, $12x + 25y = 331$

$\Longrightarrow\ 12x - 331 = -25y$

$$\Longrightarrow \quad 25|12x - 331$$

$$\Longrightarrow \quad 12x \equiv 331(mod\ 25)$$

Here $a = 12\ , b = 331\ , n = 25$

Now, $\gcd(a, n) = 1$ Then by theorem 4.7,

The linear congruence has exactly one solution.

$$12x \equiv 331(mod\ 25) \ldots\ldots\ldots.(1)$$

$$425 \equiv 0(mod\ 25)$$

$$0 \equiv 425(mod\ 25) \ldots\ldots\ldots\ldots.(2)$$

$(1) + (2) \Longrightarrow 12x \equiv 756(mod\ 25)$

$$x \equiv 63(mod\ 25)$$

Therefore, one solution is found to be $x_0 = 63$ and all other solutions is of the form $x_0 + \left(\frac{n}{d}\right)t,$ where $t = 0$.

When $t = 0\ , x = 63$

Given Diophantine equation is $12x + 25y = 331$

At (x_0, y_0), we have $12x_0 + 25y_0 = 331$

$$\Longrightarrow \quad 12 \times 63 + 25y_0 = 331$$

$$\Longrightarrow \quad 25y_0 = -425$$

$$\Longrightarrow \quad y_0 = \frac{-425}{25}$$

$$\Longrightarrow \quad y_0 = -17$$

Therefore, the solution to Diophantine equation is $x = 63$ & $y = -17$

Problem 11

Using congruences, solve the Diophantine equation below:

$5x - 53y = 17$

Solution

Given, $5x + 53y = 17$

$\Longrightarrow \quad 5x - 17 = 53y$

$\Longrightarrow \quad 53|5x - 17$

$\Longrightarrow \quad 5x \equiv 17(mod\ 53)$

Here $a = 5\ , b = 17\ , n = 53$

Now, $\gcd(a, n) = 1$

By theorem 4.11, the linear congruence has exactly one solution.

$5x \equiv 17(mod\ 53) \dots \dots \dots (1)$

$53 \equiv 0(mod\ 53)$

$0 \equiv 53(mod\ 53) \dots \dots \dots . (2)$

$(1) + (2) \Longrightarrow 5x \equiv 70(mod\ 53)$

$x \equiv 14(mod\ 53)$

Therefore, one of the solution is found to be $x_0 = 14$ and all other solutions is of the form $x_0 + \left(\frac{n}{d}\right)t,$ where $t = 0$

When $t = 0\ , x = 14$

Given Diophantine equation is $5x - 53y = 17$

At $(x_0, y_0),\ 5x_0 - 53y_0 = 17$

$\Longrightarrow \quad 5 \times 14 - 53y_0 = 17$

$\Longrightarrow \quad -53y_0 = -53$

$$\Longrightarrow \qquad y_0 = \frac{-53}{-53}$$

$$\Longrightarrow \qquad y_0 = 1$$

Therefore, the solution to diaphantine equation is $x = 14$ & $y = 1$

Problem 12

Solve each of the following sets of simultaneous congruence

$x \equiv 5(mod\ 11), x \equiv 14(mod\ 29), x \equiv 15(mod\ 31)$

Solution

Given, $x \equiv 5(mod\ 11)$

$x \equiv 14(mod\ 29)$

$x \equiv 15(mod\ 31)$

Here $a_1 = 5, a_2 = 14, a_3 = 15\ , n_1 = 11\ , n_2 = 29, n_3 = 31$

$$n = n_1 \times n_2 \times n_3$$

$$= 11 \times 29 \times 31$$

$$= 9889$$

$$N_k = \frac{n}{n_k}$$

Now, $N_1 = \frac{n}{n_1} = \frac{9889}{11} = 899$

$$N_2 = \frac{n}{n_2} = \frac{9889}{29} = 341$$

$$N_3 = \frac{n}{n_3} = \frac{9889}{31} = 319$$

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$$

$gcd(N_1, n_1) = gcd(899,11) = 1$

[∵By result gcd$(a, n) = 1$ then the linear congruence $ax \equiv b(mod\ n)$ has a unique solution]

Therefore, $899x \equiv 1(mod\ 11) \dots \dots \dots .. (1)$ has a unique solution

We have, $6292 \equiv 0(mod\ 11)$

$\Longrightarrow 0 \equiv 6292(mod\ 11) \dots \dots \dots \dots . (2)$

$(1) + (2) \Longrightarrow 899x \equiv 6292(mod\ 11)$

$$x \equiv 7(mod\ 11)$$

Therefore, one solution is $x_1 = 7$

Now, gcd$(N_2, n_2) =$ gcd$(341,29) = 1$

By theorem, $341x \equiv 1(mod\ 29) \dots \dots \dots .. (3)$ has a unique solution.

We have, $1363 \equiv 0(mod\ 29)$

$\Longrightarrow 0 \equiv 1363(mod\ 29) \dots \dots \dots \dots \dots . (4)$

$(3) + (4) \Longrightarrow 341x \equiv 1364(mod\ 29)$

$$x \equiv 4(mod\ 29)$$

Therefore, $x_2 = 4$ is a solution

Now, $gcd(N_3, n_3) = gcd(319,31) = 1$

By theorem, $319x \equiv 1(mod\ 31) \dots \dots \dots .. (5)$ has a unique solution.

$2232 \equiv 0(mod\ 31)$

$0 \equiv 2232(mod\ 31) \dots \dots \dots \dots . (6)$

$(5) + (6) \Longrightarrow 319x \equiv 2232(mod\ 31)$

$$x \equiv 7(mod\ 31)$$

Therefore, $x_3 = 7$ is a solution

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

$\quad = 5 \times 899 \times 7 + 14 \times 341 \times 4 + 5 \times 319 \times 7$

$\overline{x} = 84056$

$\overline{x} \equiv 84056(mod\ 9889)$

$\overline{x} \equiv 4944(mod\ 9889)$

Problem 13

Solve each of the following sets of simultaneous congruences

a) $x \equiv 1(mod\ 3), x \equiv 2(mod\ 5), x \equiv 3(mod\ 7)$

b) $x \equiv 51(mod\ 6), x \equiv 4(mod\ 14), x \equiv 3(mod\ 17)$

c) $2x \equiv 1(mod\ 5), 3x \equiv 9(mod\ 6), 4x \equiv 1(mod\ 7),$

$\quad 5x \equiv 9(mod\ 11)$

Solution

a) Given, $x \equiv 1(mod\ 3)$

$x \equiv 2(mod\ 5)$

$x \equiv 3(mod\ 7)$

Here $a_1 = 1, a_2 = 2, a_3 = 3\ , n_1 = 3\ , n_2 = 5, n_3 = 7$

$n = n_1 \times n_2 \times n_3$

$\quad = 3 \times 5 \times 7$

$\quad = 105$

$$N_k = \frac{n}{n_k}$$

Now, $N_1 = \frac{n}{n_1} = \frac{105}{3} = 35$

$$N_2 = \frac{n}{n_2} = \frac{105}{5} = 21$$

$$N_3 = \frac{n}{n_3} = \frac{105}{7} = 15$$

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

$gcd(N_1, n_1) = gcd(35,3) = 1$

By Corollary 4.12 we have,

$35x \equiv 1(mod\ 3) \dots\dots\dots.(1)$ has a unique solution

We have, $69 \equiv 0(mod\ 3)$

$$\Longrightarrow 0 \equiv 69(mod\ 3) \dots\dots\dots(2)$$

$(1) + (2) \Longrightarrow 35x \equiv 70(mod\ 3)$

$$x \equiv 2(mod\ 3)$$

Therefore, one of the solution is $x_1 = 2$

Now, $gcd(N_2, n_2) = gcd(21,5) = 1$

By Corollary 4.12, $21x \equiv 1(mod\ 5) \dots (3)$ has a unique solution.

We have, $20 \equiv 0(mod\ 5)$

$$\Longrightarrow 0 \equiv 20(mod\ 5) \dots\dots(4)$$

$(3) + (4) \Longrightarrow 21x \equiv 21(mod\ 5)$

$$x \equiv 1(mod\ 5)$$

Therefore, $x_2 = 1$ is a solution.

Now, gcd$(N_3, n_3) =$ gcd$(15,7) = 1$

By Corollary 4.12, $15x \equiv 1(mod\ 7) \dots (5)$ has a unique solution.

We have, $14 \equiv 0 (mod\ 7)$

$$\Longrightarrow 0 \equiv 14 (mod\ 7) \ldots \ldots \ldots (6)$$

$(5) + (6) \Longrightarrow 15x \equiv 15 (mod\ 7)$

$$x \equiv 1 (mod\ 7)$$

Therefore, $x_3 = 1$ is a solution

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$

$= 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1$

Therefore, $\overline{x} = 157$

$\Longrightarrow \overline{x} \equiv 157 (mod\ 105)$

$\Longrightarrow \overline{x} \equiv 52 (mod\ 105)$

b) Given, $x \equiv 51 (mod\ 6)$

$x \equiv 4 (mod\ 14)$

$x \equiv 3 (mod\ 17)$

Here $a_1 = 51, a_2 = 4, a_3 = 3\ , n_1 = 6\ , n_2 = 14, n_3 = 17$

$n = n_1 \times n_2 \times n_3$

$= 6 \times 14 \times 17$

$= 1428$

$$N_k = \frac{n}{n_k}$$

Now, $N_1 = \frac{n}{n_1} = \frac{1428}{6} = 238$

$$N_2 = \frac{n}{n_2} = \frac{1428}{14} = 102$$

$$N_3 = \frac{n}{n_3} = \frac{1428}{17} = 84$$

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

Now, $gcd(N_1, n_1) = gcd(238,6) = 2$

By corollary 4.12, we have,

$238x \equiv 2(mod\ 6) \dots\dots\dots..(1)$ has a unique solution

We have, $474 \equiv 0(mod\ 6)$

$$\Longrightarrow 0 \equiv 474(mod\ 6) \dots\dots\dots.(2)$$

$$(1) + (2) \Longrightarrow 238x \equiv 476(mod\ 6)$$

$$x \equiv 2(mod\ 6)$$

Therefore, one solution is $x_1 = 2$

Now, $\text{gcd}(N_2, n_2) = \text{gcd}(102,14) = 2$

By Corollary 4.12, $102x \equiv 2(mod\ 14) \dots\dots..(3)$ has a unique solution.

We have, $406 \equiv 0(mod\ 14)$

$$\Longrightarrow 0 \equiv 406(mod\ 14) \dots\dots\dots\dots(4)$$

$$(3)+(4) \Longrightarrow 102x \equiv 408(mod\ 14)$$

$$\Longrightarrow \qquad x \equiv 4(mod\ 14)$$

Therefore, $x_2 = 4$ is a solution

Now, $gcd(N_3, n_3) = gcd(84,17) = 1$

By Corollary 4.12, $84x \equiv 1(mod\ 17) \dots\dots\dots(5)$ has a unique solution.

$$1343 \equiv 0(mod\ 17)$$

$$0 \equiv 1343(mod\ 17) \dots\dots\dots\dots(6)$$

$$(5) + (6) \Longrightarrow 84x \equiv 1344(mod\ 17)$$

$$x \equiv 16(mod\ 17)$$

Therefore, $x_3 = 16$ is a solution

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$

$= 51 \times 238 \times 2 + 4 \times 102 \times 4 + 3 \times 84 \times 16$

Therefore, $\overline{x} = 29940$

$$\overline{x} \equiv 29940(mod\ 1428)$$

$$\overline{x} \equiv 48(mod\ 1428)$$

c) Given, $2x \equiv 1(mod\ 5) \ldots \ldots .. (1)$

$5 \equiv 0(mod\ 5)$

$0 \equiv 5(mod\ 5) \ldots \ldots \ldots \ldots (2)$

$(1) + (2) \Longrightarrow \quad 2x \equiv 6(mod\ 5)$

$\Longrightarrow \quad x \equiv 3(mod\ 5) \ldots \ldots \ldots .. (A)$

Given, $3x \equiv 9(mod\ 6) \ldots \ldots \ldots \ldots \ldots .. (3)$

Also, $6 \equiv 0(mod\ 6)$

$\Longrightarrow 0 \equiv 6(mod\ 6) \ldots \ldots \ldots \ldots (4)$

$(3) + (4) \Longrightarrow 3x \equiv 15(mod\ 6)$

$\Longrightarrow \quad x \equiv 5(mod\ 6) \ldots \ldots \ldots \ldots . (B)$

Given, $4x \equiv 1(mod\ 7) \ldots \ldots \ldots .. (5)$

We have, $7 \equiv 0(mod\ 7)$

$\Longrightarrow 0 \equiv 7(mod\ 7) \ldots \ldots \ldots .. (6)$

$(5) + (6) \Longrightarrow 4x \equiv 8(mod\ 7)$

$x \equiv 2(mod\ 7) \ldots \ldots \ldots .. (C)$

Given , $5x \equiv 9(mod\ 11) \ldots \ldots \ldots .. (7)$

We have, $11 \equiv 0(mod\ 11)$

$$\Longrightarrow 0 \equiv 11(mod\ 11) \ldots\ldots\ldots\ldots (8)$$

$(7) + (8) \Longrightarrow 5x \equiv 20(mod\ 11)$

$$x \equiv 4(mod\ 11) \ldots\ldots\ldots\ldots (\mathrm{D})$$

From A, B, C & D we get,

$a_1 = 3, a_2 = 5, a_3 = 2, a_4 = 4, n_1 = 5, n_2 = 6, n_3 = 7, n_4 = 11$

Therefore, $n = n_1 n_2 n_3 n_4 = 2310$

Now, $N_k = \dfrac{n}{n_k}$

$$N_1 = \frac{n}{n_1} = \frac{2310}{5} = 462$$

$$N_2 = \frac{n}{n_2} = \frac{2310}{6} = 385$$

$$N_3 = \frac{n}{n_3} = \frac{2310}{7} = 330$$

$$N_4 = \frac{n}{n_4} = \frac{2310}{11} = 210$$

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4$

$gcd(N_1, n_1) = gcd(462,5) = 1$

By Corollary 4.12, $462x \equiv 1(mod\ 5) \ldots\ldots\ldots. (9)$ has a unique solution.

We have, $1385 \equiv 0(mod\ 5)$

$$\Longrightarrow 0 \equiv 1385(mod\ 5) \ldots\ldots\ldots.. (10)$$

$(9) + (10) \Longrightarrow 462x \equiv 1386(mod\ 5)$

$$x \equiv 3(mod\ 5)$$

That is, $x_1 = 3$

Now, $gcd(N_2, n_2) = gcd(385,6) = 1$

By Corollary 4.12, $385x \equiv 1(mod\ 6) \ldots\ldots\ldots.(11)$ has a unique solution.

We have, $384 \equiv 0(mod\ 6)$

$$\Longrightarrow 0 \equiv 384(mod\ 6) \ldots\ldots\ldots\ldots\ldots(12)$$

$(11) + (12) \Longrightarrow 385x \equiv 385(mod\ 6)$

$$\Longrightarrow x \equiv 1(mod\ 6)$$

That is, $x_2 = 1$

Now, $\gcd(N_3, n_3) = \gcd(330,7) = 1$

By Corollary 4.12, $330x \equiv 1(mod\ 7) \ldots\ldots\ldots..(13)$ has a unique solution.

We have, $329 \equiv 0(mod\ 7)$

$$\Longrightarrow 0 \equiv 329(mod\ 7) \ldots\ldots\ldots\ldots.(14)$$

$(13) + (14) \Longrightarrow 330x \equiv 330(mod\ 7)$

$$x \equiv 1(mod\ 7)$$

That is, $x_3 = 1$

Now, $gcd(N_4, n_4) = gcd(210,11) = 1$

By result, $210x \equiv 1(mod\ 11) \ldots\ldots\ldots(15)$ has a unique solution.

We have, $209 \equiv 0(mod\ 11)$

$\Longrightarrow 0 \equiv 209(mod\ 11) \ldots\ldots\ldots..(16)$

$(15) + (16) \Longrightarrow 210x \equiv 210(mod\ 11)$

$$x \equiv 1(mod\ 11)$$

That is, $x_4 = 1$

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4$

$\overline{x} = 3 \times 462 \times 3 + 5 \times 385 \times 1 + 2 \times 330 \times 1 + 4 \times 210 \times 1$

$= 7583$

Hence, $\overline{x} = 7583(mod\ 2310)$

$\Longrightarrow \overline{x} = 653(mod\ 2310)$

Problem 14

Solve the linear congruence $17x \equiv 9(mod\ 276)$ using Chinese remainder theorem

Solution

Given, $17x \equiv 9(mod\ 276)$

We have, $276 = 3.4.23$

This is equivalent to finding a solution for the system of congruence

$17x \equiv 9(mod\ 3) \ldots\ldots\ldots..(1)$

$17x \equiv 9(mod\ 4) \ldots\ldots\ldots\ldots(2)$

$17x \equiv 9(mod\ 23) \ldots\ldots\ldots.(3)$

Here $n_1 = 3, n_2 = 4, n_3 = 23$

Now, $n = n_1n_2n_3$

$$N_k = \frac{n}{n_k}$$

$$N_1 = \frac{n}{n_1} = \frac{276}{3} = 92$$

$$N_2 = \frac{n}{n_2} = \frac{276}{4} = 69$$

$$N_3 = \frac{n}{n_3} = \frac{276}{23} = 12$$

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

Next we have to find the value of a_1, a_2, a_3

$(1) \Longrightarrow 17x \equiv 9(mod\ 3) \dots\dots\dots..(\text{A})$

$42 \equiv 0(mod\ 3)$

$0 \equiv 42(mod\ 3) \dots\dots\dots.(\text{B})$

$(\text{A}) + (\text{B}) \Longrightarrow 17x \equiv 51(\text{mod}\ 3)$

$x \equiv 3(mod\ 3)$

$a_1 = 3$

$(2) \Longrightarrow 17x \equiv 9(mod\ 4) \dots\dots\dots\dots.(\text{C})$

$8 \equiv 0(mod\ 4)$

$0 \equiv 8(mod\ 4) \dots\dots\dots\dots.(\text{D})$

$(\text{C}) + (\text{D}) \Longrightarrow 17x \equiv 17(\text{mod}\ 4)$

$x \equiv 1(mod\ 4)$

$a_2 = 1$

$(3) \Longrightarrow 17x \equiv 9(mod\ 23) \dots\dots\dots\dots\dots(\text{E})$

$161 \equiv 0(mod\ 23)$

$0 \equiv 161(mod\ 23) \dots\dots\dots\dots(\text{F})$

$(\text{E}) + (\text{F}) \Longrightarrow 17x \equiv 170(\text{mod}\ 23)$

$x \equiv 10(mod\ 23)$

$a_3 = 10$

Problem 15

Using congruence, solve the Diophantine equations below

a) $4x + 51y = 9$

b) $12x + 25y = 331$

c) $5x - 53y = 17$

Solution

a) Given $4x + 51y = 9$

That is, $4x \equiv 9\ (mod\ \ 51)$

$\Longrightarrow 52x \equiv\ 117(mod\ \ 51) \ldots\ldots\ldots\ldots\ldots (1)$

We have, $51x \equiv 2.51(mod\ \ 51) \ldots\ldots\ldots\ldots (2)$

Subtracting (2) from (1) we get $x \equiv\ 15(mod\ \ 51)$

Therefore $x = 15 + 51t$

Now, $51y\ \equiv 9\ (mod\ 4)$

$\Longrightarrow 17y\ \equiv 3\ (mod\ 4)$ since $\gcd(51{,}4) = 1$

$\Longrightarrow 17y - 16y\ \equiv 3\ (mod\ 4)$

$\Longrightarrow y\ \equiv\ 3\ (mod\ 4)$

Therefore, $y =\ 3 + 4s$

Hence, $4x + 51y =\ 4(15 + 51t) + 51(3 + 4s)$

$$=\ 60 + 204t + 153 + 204s$$

Therefore, $9 =\ 213 + 204t + 204s$

Which gives $-204 = 204t + 204s$

$\Longrightarrow \quad -1\ =\ t + s$

$\Longrightarrow \quad s =\ -1 - t$

Therefore, $x = 15 + 51t$ and $y = 3 + 4(-1 - t)$

$\Longrightarrow \quad y = -1 - 4t$

b) Given $12x + 25y = 331$

Then, $12x \equiv 331(mod\ 25)$

$24x \equiv 662(mod\ 25)$

Also we have, $25x \equiv 25.26(mod\ 25)$

$\Longrightarrow \quad 25x - 24x \equiv 662 - 650\ (mod\ 25)$

$\Longrightarrow \quad x \equiv 12(mod\ 25)$

Therefore, $x = 12 + 25t$

Now, $25y \equiv 331(mod\ 12)$

$\Longrightarrow \quad 25y - 24y \equiv 331 - 324\ (mod\ 12)$

$\Longrightarrow \quad y \equiv 7\ (mod\ 12)$

Therefore, $y = 7 + 12s$

Now, $12x + 25y = 12(12 + 25t) + 25(7 + 12s)$

$= 144 + 300t + 175 + 300s$

Therefore, $331 = 319 + 300t + 300s$

$\Longrightarrow 12 = 300t + 300s$

Then, $1 = 25t + 25s$

Therefore, $25t = 1 - 25s$

Now, $x = 12 + 25t$

$= 13 - 25s$

Therefore, $x = 13 - 25s$ and $y = 7 + 12s$

c) Given $5x - 53y = 17$

Therefore, $5x \equiv 17 \ (mod\ 53)$

$\Longrightarrow\ 55x \equiv 187 \ (mod\ 53)$

$\Longrightarrow 55x - 53x \equiv 187 - 3.53 \ (mod\ 53)$

$\Longrightarrow\ 2x \equiv 28 \ (mod\ 53)$

$\Longrightarrow\ x \equiv 14 \ (mod\ 53)$

Therefore, $x = 14 + 53t$

Now, $-53y \equiv 17 \ (mod\ 5)$

$\Longrightarrow\ -53y + 50y \equiv 17 \ (mod\ 5)$

$\Longrightarrow -3y \equiv 17 \ (mod\ 5)$

$\Longrightarrow -9y \equiv 51 \ (mod\ 5)$

$\Longrightarrow y \equiv 51 \ (mod\ 5)$

Therefore, $y = 51 + 5s$

Now, $5x - 53y = 5(14 + 53t) - 53(51 + 5s)$

$\Longrightarrow \qquad 17 = 70 + 265t - 2703 - 265s$

$\Longrightarrow \qquad 2650 = 265t - 265s$

Now, $\quad 10 = t - s,$

$\Longrightarrow \qquad s = t - 10$

Therefore, $y = 51 + 5(t - 10) = 5t + 1$

Therefore, $x = 14 + 53t$ and $y = 1 + 5t$

Problem 16

Obtain the two incongruent solutions $modulo$ 210 of the system

$2x \equiv 3 \ (\ mod\ 5)$

$4x \equiv 2 \ (mod \ 6)$

$3x \equiv 2 \ (mod \ 7)$

Solution

Given, $2x \equiv 3 \ (mod \ 5) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$

$4x \equiv 2 \ (mod \ 6) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$

$3x \equiv 2 \ (mod \ 7) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$

From (1) implies $4x \equiv 6 \ (mod \ 5)$

$\Longrightarrow \quad 4x - 5x \equiv 6 - 5 \ (mod \ 5)$

$\Longrightarrow \quad -x \equiv 1 \ (mod \ 5)$

$\Longrightarrow \quad x \equiv 4 \ (mod \ 5)$

From (2) implies that $\frac{4x}{2} \equiv \frac{2}{2} \left(mod \frac{6}{2}\right)$

$\Longrightarrow \quad 2x \equiv 1(mod \ 3)$

$\Longrightarrow \quad 4x \equiv 2(mod \ 3)$

$\Longrightarrow 4x - 3x \equiv 2 \ (mod \ 3)$

Therefore $x \equiv 2 \ (mod \ 6)$

Since $gcd \ (4,6) = 2,$ then the two incongruent solutions are $x_0 \ , \ x_0 + \frac{6}{2}$ where x_0 is a solution

Since $x = 2$ is a solution then $2 + \frac{6}{2} = 5$ is the other solution.

Therefore, $x \equiv 5 \ (mod \ 6)$ is the other solution.

From (3) implies, $6x \equiv 4 \ (mod \ 7)$

$\Longrightarrow 6x - 7x \equiv 4 - 7(mod7)$

$\Longrightarrow \quad -x \equiv -3(mod \ 7)$

$\Longrightarrow x \equiv 3\ (mod\ 7)$

Therefore, $x \equiv 4\ (mod\ 5)$

$x \equiv 2\ (mod\ 6)$ or $x \equiv 5\ (mod\ 6)$

$x \equiv 3\ (mod\ 7)$

Now, $N = 5.6.7 = 210$

$N_1 = 6.7 = 42$

$N_2 = 5.7 = 35$

$N_3 = 5.6 = 30$

Therefore, $42x_1 \equiv 1\ (mod\ 5)$

$\Longrightarrow \quad 42\, x_1 - 40x_1 = 1(mod\ 5)$

$\Longrightarrow \quad 2x_1 \equiv 1(mod\ 5)$

$\Longrightarrow \quad 6x_1 \equiv 3(mod\ 5)$

Then, $6x_1 - 5x_1 \equiv 3$ (mod 5)

Now, $35x_2 \equiv 1\ (mod\ 6)$

$\Longrightarrow 35\, x_2 - 36x_2 \equiv -1 + 6 = 5\ (mod\ 6)$

That is, $x_2 \equiv 5\ (mod\ 6)$

Now, $30\, x_3 \equiv 1\ (mod\ 7)$

$30\, x_3 - 28x_3 \equiv 1\ (\ mod\ 7)$ $[\because 28x_3 \equiv 0(mod\ 7)]$

$\Longrightarrow \ 2x_3 \equiv 1\ (mod\ 7)$

$\Longrightarrow \ 8x_3 \equiv 4\ (mod\ 7)$

$\Longrightarrow \ 8x_3 - 7x_3 \equiv 4\ (mod\ 7)$

Therefore, $x_3 \equiv 4\ (mod\ 7)$

Now, $a_1N_1x_1 + a_2N_2x_3 + a_3N_3x_3$

$= 4(42)(3) + 2(35)(5) + 3(30(4)$

$= 1214$

or $4(42)(3) + 5\ (35)\ (5) + 3(30)\ (4) = 1739$

Therefore, $x \equiv 1214\ (mod\ 210)$

Implies that, $x \equiv 164\ (mod\ 210\ )$

or $x = 1739\ (mod\ 210)$

Implies that, $x \equiv 59\ (mod\ 210)$.

CHAPTER - V

5.1 Fermat's Little Theorem And Pseudoprimes

Theorem 5.1 Fermat's theorem

Let p be a prime and suppose that $p \nmid a$ then $a^{p-1} \equiv 1(mod\ p)$

Proof

First we consider $p - 1$ is a positive multiples of a; that is the integers $a, 2a, 3a, 4a, \dots, (p-1)a$.

Clearly, none of this numbers is congruent to modulo p to any other, nor is any congruent to zero.

If it happens, then $ra \equiv sa(mod\ p),\ 1 \leq r < s \leq p - 1 \dots (1)$

$$\Rightarrow r \equiv s(mod\ p)$$

$$\Rightarrow p|(r - s)$$

$$\Rightarrow \ r - s > p$$

Which is contradiction to equation (1).

Hence, the previous set of integers must be congruent modulo p to $1,2,3, \dots, (p-1)$ take any some order.

Multiplying all these congruences together we find that,

$a. 2a. 3a \dots (p-1)a \equiv 1.2.3 \dots (p-1)(mod\ p)$

$\Rightarrow \ a^{p-1}\big(1.2.3 \dots (p-1)\big) \equiv 1.2.3 \dots (p-1)(mod\ p)$

$\Rightarrow \ a^{p-1}(p-1)! \equiv (p-1)!\,(mod\ p)$

We cancel $(p-1)!$ from both sides, we get $a^{p-1} \equiv 1(mod\ p)$

Corollary 5.2

If p is a prime then $a^p \equiv a(mod\,p)$

Proof

Case (i) :

Suppose $p \nmid a$ then we have p is a prime number and p does not divides a they by Fermat's theorem, $a^{p-1} \equiv 1(mod\,p)..(1)$

Also, we have $a \equiv a(mod\,p) \ldots \ldots .(2)$

Therefore $(1) \times (2) \Longrightarrow a^p \equiv a(mod\,p)$

Case (ii) :

If $p|a$ then we have, $a \equiv 0(mod\,p) \ldots \ldots (3)$

If p divides a then p divides a^p,which implies $a^p(mod\,p)..(4)$

$(3) \Longrightarrow \quad 0 \equiv a(mod\,p) \ldots .(5)$

$(4) + (5) \quad \Longrightarrow \; a^p \equiv a(mod\,p)$

Hence the proof.

Converse of Fermat's Theorem:

If $a^{n-1} \equiv 1\ (mod\ n)$ for some integer a, then n need not be prime.

Show by an illustration that the converse of the Fermat's theorem is false.

When $p = 117, a = 2$

To prove that, $a^{p-1} \not\equiv 1(mod\,p)$

That is, to prove $a^{116} \not\equiv 1(mod\,117)$

Consider, $2^{117} = 2^{7.16+5}$

$$2^{117} = (2^7)^{16}.2^5 \ldots\ldots(1)$$

We have, $2^7 = 128 \equiv 11(mod\ 117)$

$(1) \Longrightarrow\ 2^{117} \equiv 11^{16}.2^5(mod17)$

$\Longrightarrow\ 2^{117} \equiv (11^2)^8.2^5(mod17)$

$\Longrightarrow\ 2^{117} \equiv 121^8.2^5(mod17)$

$2^{117} \equiv 4^8.2^5(mod17)2^{117}$

$2^{117} \equiv (2^2)^8.2^5(mod117)2^{117}$

$2^{117} \equiv 2^{16}.2^5(mod17)2^{117}$

$2^{117} \equiv 2^{21}(mod\ 117)$

$2^{117} \equiv (2^7)^3(mod\ 117)$

$2^{117} \equiv 11^3(mod\ 117)$

$2^{117} \equiv 11^2.11(mod117)$

$2^{117} \equiv 4.11(mod\ 117)$

$2^{117} \equiv 44(mod\ 117)$

Therefore, $2^{117} \not\equiv 2(mod\ 117)$

Divided by 2, we get $2^{116} \not\equiv 1(mod\ 117)$.

So that 117 must be composite actually we have $117 = 13.9$.

Lemma: 5.3

If p and q are distinct primes with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$, then $a^{pq} \equiv a(mod\ pq)$

Proof

Given $a^p \equiv a(mod\ q) \ldots\ldots\ldots(1)$

[By corollary 5.2, if p is a prime number then $a^p \equiv a(mod\, p)$]

$(1) \Longrightarrow\ (a^p)^q \equiv a^p(mod\, q)$

$\Longrightarrow\ a^{pq} \equiv a^p(mod\, q) \dots\dots..(2)$

Combining the congruence (1) & (2) we get, $a^{pq} \equiv a(mod\, q)$

[$\because$ If $a \equiv b(mod\, n)$ and $b \equiv c(mod\, n)$ then $a \equiv c(mod\, n)$]

$\Longrightarrow\ q|(a^{pq} - a) \dots\dots..(3)$

Given, $a^q \equiv a(mod\, p) \dots\dots.(4)$

Again by corollary 5.2, we get $(a^q)^p \equiv a^q(mod\, p)$

$\Longrightarrow a^{qp} \equiv a^q(mod\, p) \dots\dots(5)$

Combining the congruence (4) & (5) we get $a^{qp} \equiv a(mod\, p)$

$\Longrightarrow\ p|(a^{pq} - a) \dots\dots.(6)$

By corollary, we have [If $a|c\ and\ b|c$ with $gcd(a, b) = 1$ then $ab|c$]

Therefore from (3) and (6) we get, $pq|(a^{pq} - a)$

$\Longrightarrow\ \ a^{pq} \equiv a(mod\, pq)$

Definition *Pseudo Prime*

A composite integer n is called pseudo prime whenever $n|2^n - 2$

Note

There are infinitely many pseudo primes. The smallest four being $341, 561, 645, 1105.$

Theorem: 5.4

If n is an odd pseudo prime then $M_n = 2^n - 1$ is the larger one.

Proof

Let n be a odd pseudo prime.

$\Longrightarrow$ n is a composite number.

We can write $n = rs$ with $1 < r \leq s < n$

$\Longrightarrow$ $r|n$

$\Longrightarrow$ $(2^r - 1)|(2^n - 1)$

$\Longrightarrow$ $(2^r - 1)|M_n \ldots\ldots\ldots(1)$

Also given, n is the odd pseudo prime.

Then by definition, $n|2^n - 2$

$\Longrightarrow$ $2^n - 2 = kn, \quad k \in z \ldots\ldots\ldots\ldots.(2)$

It follows that $2^{M_n} = 2^{2^n - 1}$

$\Longrightarrow$ $2^{M_n - 1} = 2^{2^n - 1 - 1}$

$\Longrightarrow$ $2^{M_n - 1} = 2^{2^n - 2}$

$\Longrightarrow$ $2^{M_n - 1} = 2^{kn} \qquad [\, by\ (2)]$

$\Longrightarrow$ $2^{M_n - 1} - 1 = 2^{kn} - 1$

$\Longrightarrow$ $2^{M_n - 1} - 1 = (2^n)^k - 1$

Therefore, $2^{M_n - 1} - 1 = (2^n - 1)\big[2^{n(k-1)} + 2^{n(k-2)} + \cdots +$

2n+1

[Formula : $x^k - 1 = (x - 1)[x^{k-1} + x^{k-2} + \cdots + x + 1]$

$\Longrightarrow$ $2^{M_n - 1} - 1 = M_n\big[2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\big]$

$\Longrightarrow$ $2^{M_n - 1} - 1 \equiv 0(mod\ M_n)$

$\Longrightarrow$ $2^{M_n}.2^{-1} - 1 \equiv 0(mod\ M_n)$

$$\Longrightarrow \frac{2^{M_n}}{2} - 1 \equiv 0(mod\ M_n)$$

$$\Longrightarrow \frac{2^{M_n} - 2}{2} \equiv 0(mod\ M_n)$$

$$\Longrightarrow 2^{M_n} - 2 \equiv 0(mod\ M_n)$$

$$\Longrightarrow M_n | 2^{M_n} - 2$$

Hence, by the definition of pseudo prime M_n is a pseudo prime.

Definition

A composite integers n for which $a^n \equiv a(mod\, n)$ is called a **pseudo prime to the base $\boldsymbol{a}$** (When $a = 2$, n is simply said to be pseudo prime).

Result

1) 91 is the smallest pseudo prime to the base 3

2) 207 is the smallest pseudo prime to the base 5

Result

There exists composite number n that are pseudo primes to every base a that is, $a^n \equiv a(mod\ n)$ for all integers a.

The least pseudo prime 561,341,645 and 1105. These exceptional numbers are called **absolute pseudo primes (or) Carmichael number**.

PROBLEMS 5.1

Problem: 1

Use Fermat's theorem to verify that 17 divides $11^{104}+1$

Solution

Since 17 does not divides 11, we have, $11^{16} \equiv\ 1\ (mod 17)$

Therefore, $(11^{16})^6\ =\ 11^{96} \equiv 1\ (mod\ 17)$

But $121\ =\ 11^2$ and $7.17 = 119 = 121 - 2$

Therefore, $11^2 \equiv\ 2\ (mod\ 17)$

Hence $11^2 \equiv\ 2^4\ = 16\ (mod\ 17)$ and

$11^{96}.11^8 \equiv 16\ (mod\ 17$

$\Longrightarrow\ 11^{104}\ \equiv 16\ (mod\ 17)$

But $16 \equiv\ -1\ (mod\ 17)$

Therefore, $11^{104}\ \equiv\ -1\ (mod\ 17)$

This gives $17|11^{104}+1$.

Problem 2

If $gcd(a,30) = 1$ then show that 60 divides $a^4 + 59$

Solution

Assume that $gcd\ (a,30) = 1$.

We have to show that $60|\mathrm{a}^4 + 59$.

Now, $gcd(a,30) = 1$ implies that

$gcd(a,2) = gcd(a,3) = gcd(a,5) = 1$

Also, $gcd(a,4)\ = gcd(a,2^2) = 1$

Also we have, $60 = 2^2.3.5$.

Now, $60|(\mathrm{a}^4+59)$ is the same as $a^4 \equiv -59\ (mod 60)$ or

$a^4 \equiv 1(mod\ 60)$

Since, $gcd(a,5)=1$ implies that $a^4 \equiv 1(mod\ 5)$.

Also, $gcd\ (a,3)=1 \Longrightarrow a^4 \equiv 1(mod\ 3)$.

Again, $gcd(a,2)=1 \Longrightarrow a \equiv 1\ (mod 2)$

Therefore, $a^2 \equiv 1(mod\ 2)$

Also, $a^2 \equiv 1-2=-1\ (mod\ 2)$

Therefore, $2|(a^2-1)$, $2|(a^2+1)$ implies that

$4|(a^2+1)(a^2-1)=a^4-1$

Hence, we get $5|(a^4-1)$, $3|(a^4-1)$, $4|(a^4-1)$ and

$gcd(5,a)=gcd(3,a)=gcd(4,a)=1$.

Therefore, $60|(a^4-1)$

Hence, $a^4 \equiv 1\ (mod\ 60)$, $a^4 \equiv 1-60=-59\ (mod\ 60)$

Therefore, $60|(a^4+59)$

Problem 3

If 7 does not divides a, prove that either a^3+1 or a^3-1 is divisible by 7

Solution

Assume that 7 does not divides a, then prove that $7|(a^3+1)$ or $7|(a^3-1)$.

By Fermat's theorem, we have $a^6 \equiv 1(mod\ 7)$

Therefore, $7|(a^6-1)$.

But $a^6-1=(a^3+1)(a^3-1)$

Suppose 7 does not divides $a^3 + 1$ then, $gcd\ (7, a^3 + 1) = 1$ and so by Euclid's lemma we have $7|a^3 - 1$

Problem 4

Confirm that the following integers are absolute pseudoprimes

a) $1105 = 5.13.17$

b) $2821 = 7.13.31$

c) $2465 = 5.17.29$

Solution

a) Given, $1105 = 5.13.17$

Let a be any integer

If 1105 does not divides a, then, 5 does not divides a, 13 does not divides a,17 does not divides a .

Therefore, by Fermat's theorem,

$a^4 \equiv 1(mod\ 5)$, $a^{12} \equiv 1(mod\ 13)$ and $a^{16} \equiv 1\ (mod\ 17)$

Therefore, $a^{1104} = (a^4)^{276} \equiv 1\ (mod\ 5)$

$\Longrightarrow\ a^{1104} = (a^{12})^{92} \equiv 1(mod\ 13)$

$\Longrightarrow\ a^{1104} = (a^{16})^{69} \equiv 1(mod\ 17)$

Hence, $a^{1104} \equiv 1\ (mod\ 5.13.17)$ when 1105 does not divides a and, $a^{1105} \equiv a\ (mod\ 1105)$ when 1105 does not divides a.

But when $1105|a$, clearly $1105|\ (a^{1105} - a)$

Therefore, $a^{1105} \equiv a(mod\ 1105)$ for all a.

b) Given $2821 = 7.13.31$

Let a be any integer.

If 2821 does not divides a, then 7 does not divides a, 13 does not divides a, 31 does not divides a.

Therefore, $a^6 \equiv (mod\ 7)$, $a^{12} \equiv (mod\ 13)$ and

$a^{13} \equiv 1(mod\ 31)$

Also, $a^{2820} = (a^6)^{470} \equiv 1\ (mod\ 7)$

$\Longrightarrow\ a^{2820} = (a^{12})^{235} \equiv 1\ (mod\ 13)$

$\Longrightarrow\ a^{2820} = (a^{30})^{94} \equiv 1\ (mod\ 31)$

Therefore, $a^{2820} \equiv 1\ (mod\ 7.13.31)$ when 2821 does not divides a.

Hence, $a^{2821} \equiv a\ (mod\ 2821)$ when 2821 does not divides a.

But when $2821|a$, clearly $a^{2821} \equiv a\ (mod\ 2821)$

Therefore, for all a, $a^{2821} \equiv a\ (mod\ 2821)$

c) Given, $2461 = 5.17.29$

Let a be any integer.

If 2465 does not divides a, then, 5 does not divides a, 17 does not divides a, and 29 does not divides a.

Therefore, $a^4 \equiv 1(mod\ 5)$, $a^{16} \equiv 1\ (mod\ 17)$, and

$a^{28} \equiv 1\ (mod\ 29)$

Now, $a^{2464} = (a^4)^{616} \equiv 1\ (mod\ 5)$

$\Longrightarrow\ a^{2464} = (a^{16})^{154} \equiv 1\ (mod\ 17)$

$\Longrightarrow\ a^{2464} = (a^{28})^{88} \equiv 1\ (mod\ 29)$

Therefore, $a^{2464} \equiv 1\ (mod\ 5.17.29)$ when 2465 does not divides a and $a^{2465} \equiv\ a\ (mod\ 2465)$ when 2465 does not divides a.

But when $2465|a$, clearly $a^{2465} \equiv\ a\ (mod\ 2465)$.

Therefore, for all a, $a^{2465} \equiv\ a\ (mod\ 2465)$.

Problem 5

Prove the following:

a) If $gcd(a, 35) = 1$, show that $a^{12} = 1(mod\ 35)$.

b) If $gcd(a, 42) = 1$, show that $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.

c) If $gcd(a, 133) = gcd(b, 133) = 1$,

show that $133|a^{18} - b^{18}$.

Solution

a) Given $gcd(a, 35) = 1$.

We have $35 = 7.5$, then $gcd(a, 7) = 1$ and $gcd(a, 5) = 1$.

Therefore, by Fermat's theorem, $a^6 \equiv 1(mod\ 7)$ and $a^4 \equiv 1(mod\ 5)$.

Hence, $a^{12} = a^6 a^6 \equiv 1(mod\ 7) \Longrightarrow 7|(a^{12} - 1)$ and $a^{12} = (a^4)^3 \equiv 1(mod\ 5)$

$\Longrightarrow\ 5|(a^{12} - 1)$.

Since $gcd(5,7) = 1$ we have, by corollary 2.7 we have $35|(a^{12} - 1)$.

Which implies $a^{12} \equiv 1(mod\ 35)$.

b) Given $gcd(a, 42) = 1$.

We have $42 = 7.3.2$,then $gcd(a, 7) = 1$, $gcd(a, 3) = 1$ and $gcd(a, 2) = 1$

Therefore, by Fermat's theorem, $a^6 \equiv 1(mod\ 7)$, $a^2 \equiv 1(mod\ 3)$ and $a \equiv 1(mod\ 2)$

Now, $a^2 \equiv 1(mod\ 3) \implies (a^2)^3 = a^6 \equiv 1(mod\ 3)$

Therefore, $a^6 \equiv 1(mod\ 3)$.

Also, we have $a^6 - 1 = (a-1)(a^5 + a^4 + a^3 + a^2 + a + 1)$

$$= (a-1)[a^3(a^2 + a + 1) + a^2 + a + 1]$$

$$= (a-1)(a^3 + 1)(a^2 + a + 1)$$

$$= (a-1)(a+1)(a^2 - a + 1)(a^2 + a + 1)$$

Since, a is odd and if $a > 0$ then $a \geq 3$ so $2|(a-1)$ and $4|(a+1)$.

Therefore, $8|(a^6 - 1)$.

If $a < 0$ then $a \leq 3$ so $4|(a-1)$ and $2|(a+1)$.

Therefore, $8|(a^6 - 1)$.

Hence, we have $7|(a^6 - 1)$, $3|(a^6 - 1)$ and $8|(a^6 - 1)$.

Also, we have 3,7,8 are relatively prime.

Hence, $3.7.8 = 168|(a^6 - 1)$.

c) Given $gcd(a, 133) = gcd(b, 133) = 1$.

We have $133 = 7.19$, then $gcd(a, 7) = gcd(b, 7) = 1$ and $gcd(a, 19) = \text{gcd}(b, 19) = 1$.

Therefore, by Fermat's theorem,

$a^6 \equiv 1(mod\ 7)$, $b^6 \equiv 1(mod\ 7)$ and

$a^{18} \equiv 1(mod\ 19)$, $b^{18} \equiv 1(mod\ 19)$

Therefore, $a^6 - b^6 \equiv 1 - 1 = (mod\ 7) \implies 7|a^6 - b^6$

And $a^{18} - b^{18} \equiv 1 - 1 = (mod\ 19) \implies 19|a^{18} - b^{18}$.

Since, $a^{18} - b^{18} = (a^6)^3 - (b^6)^3$

$$= (a^6 - b^6)[(a^6)^2 + a^6b^6 + (b^6)^2]$$

then $7|a^{18} - b^{18}$.

Therefore, $7.19 = 133|(a^{18} - b^{18})$

Problem 6

From Fermat's theorem deduce that, for any integer ≥ 0, $13|11^{12n+6} + 1$.

Solution

Since $13 \nmid 11$ by Fermat's theorem we have,

$11^{12} \equiv 1(mod\ 13)$.

Therefore, $11^{12n} \equiv 1^n = 1(mod\ 13)$.

But $11^2 = 121$ and $9.18 = 117$.

Therefore, $11^2 \equiv 4(mod\ 13) \implies 11^6 \equiv 4^3 = 64(mod\ 13)$.

$\implies 11^6 \equiv 64 - 13.5 \equiv -1(mod\ 13$.

Therefore, $11^{12n}.11^6 \equiv 1^n.(-1) = -1(mod\ 13)$.

Hence, $11^{12n+6} \equiv -1(mod\ 13)$.

Therefore, $13|11^{12n+6} + 1$.

Problem 7

Prove that if p is an odd prime and k is an integer satisfying $1 \leq k \leq p-1$, then the binomial coefficient $\binom{p-1}{k} \equiv (-1)^k (mod\, p)$.

Proof

We have $\binom{p-1}{k} = \frac{(p-1)!}{k!\,(p-k)!} = \frac{(p-1)(p-2)\ldots(p-k)}{k!}$

Therefore, $k!\binom{p-1}{k} \equiv (p-1)(p-2)\ldots(p-k)$

But $p-j \equiv -j(mod\, p)$.

Therefore,

$$\begin{aligned}(p-1)(p-2)\ldots(p-k) &\equiv (-1)(-2)\ldots(-k)(mod\, p)\\ &\equiv (-1)^k k!\,(mod\, p).\end{aligned}$$

Therefore, $k!\binom{p-1}{k} \equiv (-1)^k k!\,(mod\, p)$.

Since, $p-1 \geq k, p > k$ then $p \nmid 1.2.3\ldots k = k!$ then by corollary 4.5 we have $\binom{p-1}{k} \equiv (-1)^k (mod\, p)$.

Problem 8

Assume that p and q are distinct odd primes such that $p-1|q-1$. If $gcd(a\,,pq) = 1$, show that $a^{q-1} = 1\ (mod\, pq)$

Solution

Given, p and q are distinct odd primes such that $p-1|q-1$

Which implies $q-1 = k(p-1)$ for some k

Also, given $gcd(a\ ,pq) = 1 \Longrightarrow \gcd(a,p) = \gcd(a,q) = 1$

Therefore, $a^{p-1} \equiv 1(mod\ p)$ and $a^{q-1} \equiv 1(mod\ q)$

Now, $a^{p-1} \equiv 1(mod\ p)\ \Longrightarrow a^{k(p-1)} \equiv 1^k(mod\ p)$

$\Longrightarrow\ a^{q-1} \equiv 1(mod\ p)$.

Therefore, $p|a^{q-1}$ and $q|a^{q-1}$.

Then by corollary 2.7, we have, $pq|a^{q-1}$.

Hence, $a^{q-1} = 1\ (mod\ pq)$.

Problem 9

If p and q are distinct primes, prove that

$p^{q-1} + q^{p-1} = 1(mod\ pq)$.

Solution

Given, p and q are distinct primes then by Fermat's theorem $p^{q-1} \equiv 1(mod\ q)$.

We have $q|q^{p-1}$ so $q^{p-1} \equiv 0(mod\ q)$

Therefore, $p^{q-1} + q^{p-1} \equiv 1(mod\ q)$

Similarly, $p|p^{q-1}$ so $p^{q-1} \equiv 0(mod\ p)$ and $q^{p-1} \equiv 1(mod\ p)$

Therefore, $p^{q-1} + q^{p-1} \equiv 1(mod\ p)$

Hence, we have $p|p^{q-1} + q^{p-1} - 1$ and $q|p^{q-1} + q^{p-1} - 1$ and $gcd(p,q) = 1$

Therefore, by a corollary 2.7 we have, $pq|p^{q-1} + q^{p-1} - 1$

Which implies $p^{q-1} + q^{p-1} = 1(mod\ pq)$

Problem 10

Show that $2222^{5555} + 5555^{2222} \equiv 0(mod\ 7)$.

Solution

We have, $1111 = 159.7 - 2$ therefore $1111 \equiv -2(mod\ 7)$.

Therefore, $2222 \equiv -4(mod\ 7)$ and $5555 \equiv -10 \equiv -10 + 14 \equiv 4(mod\ 7)$.

Hence, $2222^{5555} \equiv (-4)^{5555}(mod\ 7)$.

But $(-4)^2 = 16 \equiv 2(mod\ 7)$ and $5555 = 2(2777) + 1$.

Therefore, $(-4)^{5555} = (-4)^{2(2777)+1} \equiv 2^{2777}(-4)(mod\ 7)$.

Hence, $2222^{5555} \equiv -2^{2779}(mod\ 7)$.

But $2^3 \equiv 1(mod\ 7)$ and $3.926 = 2778$.

Therefore, $(2^3)^{926} \equiv 2^{2778} \equiv 1(mod\ 7)$

Hence, $2222^{5555} \equiv -2^{2779} = -2^{2778}.2 \equiv -2(mod\ 7) \ldots$ (1)

Now, $5555 \equiv 4(mod\ 7) \implies 5555^{2222} \equiv 4^{2222}(mod\ 7)$.

Therefore, $5555^{2222} \equiv 2^{4444}(mod\ 7)$ and $4444 = 1481.3 + 1$.

Hence, $5555^{2222} \equiv 2^{1481.3+1}(mod\ 7)$

$\implies 5555^{2222} \equiv (2^3)^{1481}.2(mod\ 7)$

But we have, $2^3 \equiv 1(mod\ 7)$.

Therefore, $5555^{2222} \equiv 1.2 = 2(mod\ 7) \ldots\ldots.(2)$

Hence, $2222^{5555} + 5555^{2222} \equiv -2 + 2 = 0(mod\ 7)$.

5.2 Wilson's Theorem

Theorem 5.4 *Wilson*

If p is a prime number then $(p-1)! \equiv -1(mod\ p)$

Proof

Let p be a prime number.

Dismissing the cases $p = 2, p = 3$ as being obviously true.

Therefore let us take $p > 3$

Suppose that a is any one of the $p-1$ positive integers $1,2,3,\dots,p-1$ and consider the linear congruence $ax \equiv 1(mod\, p)$.

Then $gcd(a,p) = 1$.

Then by theorem, $ax \equiv 1(mod\, p)$ has a unique solution. [∵ If $gcd(a,n) = 1$ then the linear congruence $ax \equiv 1(mod\, n)$ has a unique solution]

Hence there is a unique integers $a^{'}$ with $1 \le a^{'} \le p-1$ satisfying $aa^{'} \equiv 1(mod\, p) \dots\dots\dots (1)$

Because p is a prime, $a = a^{'}$ iff $a = 1$ or $a = p-1$

Assume that, $a = a^{'}$

$(1) \Longrightarrow\ a^2 \equiv 1(mod\, p)$

$\Longrightarrow\ a^2 - 1 \equiv 0(mod\, p)$

$\Longrightarrow\ (a-1)(a+1) \equiv 0(mod\, p)$

Therefore, either $a - 1 \equiv 0(mod\, p)$ in which case $a = 1$ or $a + 1 \equiv 0(mod\, p)$ in which case $a = p-1$.

If we omit the number 1 and $p-1$ the effect is to group the remaining integers $2,3,\dots,p-2$ into pairs $a, a^{'}$ where $a \neq a^{'}$, such that their product $aa^{'} \equiv 1(mod\, p)$

When these $\frac{p-3}{2}$ congruence are multiple together and the factors rearranged we get, $2.3 \ldots \ldots . p-2 \equiv 1(mod\, p)$

$\Longrightarrow (p-2)! \equiv 1(mod\, p)$

Multiply on both sides by $p-1$ we get,

$(p-1)(p-2)! \equiv (p-1)(mod\, p)$

$\Longrightarrow (p-1)! \equiv -1(mod\, p)$

Example for the Wilson's Theorem:

Let us take $p = 13$

It is possible to divide the integers $2,3,4, \ldots \ldots ..$ into

$\frac{p-3}{2} = \frac{13-3}{2} = 5$ pairs.

Each product of which is congruent *1* modulo *13*

Therefore we can write $2.7 \equiv 1(mod\ 13)$

$3.9 \equiv 1(mod\ 13)$

$4.10 \equiv 1(mod\ 13)$

$5.8 \equiv 1(mod\ 13)$

$6.11 \equiv 1(mod\ 13)$

Multiply all these congruence,

we get $2.3.4.5.6.7.8.9.10.11 \equiv 1(mod\ 13)$

Which implies, $11! \equiv 1(mod\ 13)$

Multiply on both sides by 12 we get, $12.11! \equiv 12(mod\ 13)$

$\Longrightarrow\ 12! \equiv 12(mod\ 13)$

$\Longrightarrow\ 12! \equiv -1(mod\ 13)$

Result

The converse of Wilson's theorem is also true. That is if $(n-1)! \equiv -1(mod\ n)$ then n must be a prime number.

Proof

Suppose n is not a prime

Then, n must be a composite number.

Hence, n has a divisor d with $1 < d < n$

Further more $d \leq n-1$, d occurs one of the factors in $(n-1)!$

Therefore $d|(n-1)!$

Assume that, $(n-1)! \equiv -1(mod\ n)$

$\Longrightarrow\ n|(n-1)! + 1$

$\Longrightarrow d|(n-1)! + 1$

$\Longrightarrow d|(n-1)!$ or $d|$

Therefore $d|1$ is impossible.

Which implies n is a prime number.

Hence $(n-1)! \equiv -1(mod\ n)$ then n must be prime number.

Theorem: 5.5

The quadratic congruence $x^2 + 1 \equiv 0(mod\ p)$ where p is an odd prime has a solution if and only if $p \equiv 1(mod\ 4)$

Proof

Assume that the quadratic congruence $x^2 + 1 \equiv 0(mod\ p)$ has a solution say 'a'

Therefore $a^2 + 1 \equiv 0(mod\ p)$

$\Longrightarrow\ a^2 \equiv -1(mod\ p) \dots\dots\dots.(1)$

Given p is an odd prime number then $p \nmid a$.

Then by Fermat's Theorem $a^{p-1} \equiv 1(mod\ p)$

$\Longrightarrow 1 \equiv a^{p-1}(mod\ p)$ $\quad$ [$\because If\ a \equiv b(mod\ n)$ then $b \equiv a(mod\ n)$]

$\Longrightarrow 1 \equiv a^{2\left(\frac{p-1}{2}\right)}(mod\ p)$

$\Longrightarrow 1 \equiv -1^{\left(\frac{p-1}{2}\right)}(mod\ p) \dots\dots\dots\dots(2)$

Since p is an odd prime.

Therefore, p is of the form either $4k+1$ or $4k+3$.

Suppose p is an odd prime then $p = 4k+3$.

Consider, $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}}$

$= (-1)^{\frac{4k+2}{2}}$

$= -1$

Therefore $(2) \Longrightarrow \quad 1 \equiv -1(mod\ p)$

$\Longrightarrow \quad p|2$

Which is a contradiction (since p is an odd prime)

Therefore p is of the form $4k+1$

That is $p = 4k+1$

$\Longrightarrow p - 1 = 4k$

Therefore $p \equiv 1(mod\ 4)$ $\quad$ [$\because\ If\ a - b = kn,$ then $a \equiv b(mod\ n)$]

Conversely, assume that $p \equiv 1(mod\ 4)$ then $p = 4k+1$ for some k.

In the product, $(p-1)! = 1.2.3 \ldots \frac{p-1}{2}\frac{p+1}{2} \ldots .(p-2)(p-1)$

We have the congruence,

$$p-1 \equiv -1(mod\, p)$$

$$p-2 \equiv -2(mod\, p)$$

$$\begin{matrix} . & . & . \\ . & . & . \\ . & . & . \end{matrix}$$

$$\frac{p+1}{2} \equiv \frac{-(p-1)}{2}(modp)$$

Rearranging the factors,

$$(p-1)! \equiv 1.(-1).2(-2) \ldots ..\left(\frac{p-1}{2}\right).\left(\frac{-(p-1)}{2}\right)(mod\, p)$$

$$\Longrightarrow \quad (p-1)! \equiv (-1)^{\frac{p-1}{2}}\left(1.2.3 \ldots \frac{p-1}{2}\right)^2 \ (mod\, p),$$

since there are $\frac{p-1}{2}$ minus signs involved.

Therefore, $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 (mod\, p)$

By Wilson's Theorem, we have $(p-1)! \equiv -1(mod\, p)$

Therefore $(-1) \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 (mod\, p) \ldots \ldots \ldots \ldots \ldots (3)$

We assume that p is of the form $4k+1$

Consider, $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}}$

$$= (-1)^{2k} = 1$$

Therefore (3) $\Longrightarrow \ -1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (mod\, p)$

$$\Rightarrow \quad 0 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1(mod\ p)$$

$$\Rightarrow \quad \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0(mod\ p)$$

Take $x = \left(\frac{p-1}{2}\right)!$ then, we have $x^2 + 1 \equiv 0(mod\ p)$

Therefore, the integer $\left(\frac{p-1}{2}\right)!$ satisfies the quadratic congruence, $x^2 + 1 \equiv 0(mod\ p)$.

PROBLEMS 5.2

Problem 1

Find the remainder when $15!$ Is divided by 17

Solution

Let 17 be a prime number.

Then by Wilson’s theorem $(17-1)! \equiv -1\ (mod\ 17)$

Which implies, $16! \equiv -1\ (mod\ 17)$.

But $16 \equiv -1\ (mod\ 17)$.

Therefore, $16! \equiv 16\ (mod\ 17)$ and $gcd(16,17) = 1$.

Hence, $16!|16 \equiv 16|16\ (mod\ 17)$.

Which gives $15! \equiv 1\ (mod\ 17)$

Problem 2

Find the remainder when $2(26!)$ is divided by 29.

Solution

Given 29 is a prime number.

Then by Wilson's theorem, $28! \equiv -1\ (mod\ 29)$

Since $gcd\ (28,29) = 1$ Therefore, we have $27! \equiv 1(mod\ 29)$

$\Longrightarrow 27! \equiv 1 + 29$ (mod 29).

Therefore, $27! \equiv 30\ (mod\ 29) \Longrightarrow 9.3.26! \equiv 30(mod\ 29)$

Also, $9.26! \equiv 10\ (mod\ 29)$.

Since, $gcd(3,29) = 1$.

Therefore, $9.26! \equiv 39\ (mod\ 29) \Longrightarrow 3.26! \equiv 13\ (mod\ 29)$

Hence, $3.26! \equiv 13 + 21 = 42 = 3.14\ (mod\ 29)$.

That is, $26! \equiv 14\ (mod\ 29)$.

Therefore, $2.26! \equiv 28\ (mod\ 29)$

Problem 3

Show that $18! \equiv -1\ (mod\ 437)$

Solution

To prove that, $18! \equiv -1\ (mod\ 437)$

Since $19.23 = 437$ we have $19|437$

By Wilson's theorem, we have $18! \equiv -1\ (mod\ 19)$

We must show that $23|(18! + 1)$

By Wilsons theorem, $22! \equiv -1 \equiv 22\ (mod\ 23)$

Therefore, $22!|22 \equiv 22|22 = 1\ (mod\ 23),$

Therefore $gcd(22,23) = 1$

Also, $21! \equiv 1 \equiv 1 + 23 = 24\ (mod\ 23)$

$\Longrightarrow 21.20! \equiv 8.3\ (mod\ 23)$

Hence, $7.20! \equiv 8\ (mod\ 23)$,

Therefore $gcd\ (3{,}23) = 1$

Now, $7.20.19! \equiv 8\ (mod\ 23)$

$\Longrightarrow 7.5.19! \equiv 2\ (mod\ 23)$

Therefore $gcd\ (4{,}23)$

Also, $7.5.19.18! \equiv 2\ (mod\ 23)$

Therefore, $7.5.19.18! \equiv 2 + 23 = 25\ (mod\ 23)$

Hence, $7.19.18! \equiv 5\ (mod\ 23)$,

Therefore $gcd\ (5{,}23) = 1$.

And $7.19.18! \equiv 5 + 23 = 28\ (mod\ 23)$

$\Longrightarrow 19.18! \equiv 4\ (mod\ 23)$,

Therefore $gcd(7{,}23) = 1$

And $19.18! \equiv 4 - 23 = -19(mod\ 23)$

$\Longrightarrow 18! \equiv -1\ (mod\ 23)$

Therefore $gcd(19{,}23) = 1$

Hence, $23|(18! + 1)$ and $19|(18! + 1)$

Therefore, $19.23 = 437|(18! + 1)$

Problem 4

Find two odd primes $\mathrm{p} \leq 13$ for which thee congruence $(\mathrm{p} - 1)! \equiv -1\ (\mathrm{mod}\ \mathrm{p}^2)$ holds.

Solution

When $\mathrm{p} = 5$, we have $4! + 1 = 25$

So that, $\mathrm{p}^2|(\mathrm{p} - 1)! + 1$

When $\mathrm{p} = 7$, we have $6! + 1 = 721$

Which implies, 7^2 does not divides 721

When p $= 9$, we have, $8! + 1 = 40321$,

$\Longrightarrow$ 9 does not divides 40321

When p $= 11$, we have, $10! + 1 = 3{,}628{,}801$,

$\Longrightarrow$ 11^2 does not divides 3628801

When p $= 13$, we have, $12! + 1 = 479001601$

$\Longrightarrow$ $13^2|479001601$

Problem 5

Verify that $4(29!) + 5!$ Is divisible by 3!

Solution

By Wilsons theorem, $30! \equiv -1\ (mod\ 31)$

Therefore, $30.29! \equiv 31 - 1 = 30\ (mod\ 31)$

Hence $29! \equiv 1\ (mod\ 31)$ as $gcd(30{,}31) = 1.$

Therefore, $4(29!) \equiv 4\ (mod\ 31)$

We know that, $5! = 120$

Then, $4(29!) + 5! \equiv 4 + 120$

$$= 124(mod\ 31)$$

But $124 = 4.31$

Therefore, $4(29!) + 5! \equiv 0\ (mod\ 31)$

Which gives $31|[4(29!) + 5!]$

Problem 6

Prove that if p and p $+ 2$ are a pair of twin primes, then

$4((p - 1)! + 1) + p \equiv 0\ (mod\ p(p + 2))$

Solution

By Wilsons theorem, $(p-1)! \equiv -1\ (mod\ p)$

Therefore, $(p-1)!+1 \equiv 0\ (mod\ p)$

Hence $4[(p-1)!+1] \equiv 0\ (mod\ p)$

$\Longrightarrow 4[(p-1)!+1]+p \equiv 0\ (mod\ p) \ldots\ldots\ldots..(1)$

Now, $(p+2-1)! = (p+1)! \equiv -1\ (mod\ (p+2))$

[by Wilson's theorem]

Therefore, $(\mathrm{p}+1)\mathrm{p}! \equiv -1+\mathrm{p}+2$

$= p+1\ (mod\ (p+2))$

Then, $p! \equiv 1\ (mod\ (p+2))$ as $gcd(p+1, p+2) = 1$

Therefore, $4\mathrm{p}! \equiv 4 = 4+2\mathrm{p}-2\mathrm{p}$

$= 2(p+2)-2p\ (mod\ (p+2))$

Hence, $4p(p-1)! \equiv -2p\ (mod\ (p+2))$

Therefore, $4(p-1)! \equiv -2\ (mod\ (p+2))$, as $gcd(p, p+2) = 1$

Then, $4(p-1)! + p + 2 \equiv -2\ (mod\ (p+2))$ and

$4(p-1)! + p + 4 \equiv 0\ (mod\ (p+2))$

Therefore, $4[(p-1)!+1]+p \equiv 0\ (mod\ (p+2) \ldots\ldots..(2)$

Hence, p and $p+2$ divide $4[(p-1)!+1]+p$

[by equation (1) & (2)]

Which gives $p(p+2)$ divides $4[(p-1)!+1]+p$

Therefore, $4[(p-1)!+1]+p \equiv 0\ (mod\ p(p+2))$

Problem 7

Given prime number p, establish the following congruence

$(p-1)! \equiv p-1(mod\ 1+2+3+\cdots+(p-1))$.

Solution

When $p=2$, the result is obvious. So we can take $p>2$.

From Wilson's theorem we have $(p-1)! \equiv -1(mod\ p)$.

Which implies, $(p-1)! \equiv -1 \equiv -1+p(mod\ p)$.

Therefore, $p|(p-1)!-(p-1)$

We have, $1+2+3+\cdots+(p-1)=\frac{(p-1)p}{2}$

Since $p>2$ is a prime number then $p-1$ is even therefore

$\frac{(p-1)}{2}$ is an integer and $\frac{(p-1)}{2}<p-1$

Also we have, $p-1|(p-1)!-(p-1)$

Therefore, $\left(\frac{p-1}{2}\right)|(p-1)!-(p-1)$

Since, p is prime we have $gcd\left(\frac{p-1}{2},p\right)=1$

Which implies, p and $\frac{p-1}{2}$ divides $(p-1)!-(p-1)$

So $\frac{(p-1)p}{2} = 1+2+3+\cdots+\big(p-1\big)$ divides

$(p-1)!-(p-1)$

Therefore, $(\mathrm{p}-1)! \equiv \mathrm{p}-1(\mathrm{mod}\ 1+2+3+\cdots+(\mathrm{p}-1))$.

Problem 8

If p is a prime, prove that for any integer a,

a) $p|a^p + (p-1)!\,a$

b) $p|(p-1)!\,a^p + a$

Solution

a) Let p be a prime number.

By a corollary 5.2 we have $a^p \equiv a(mod\ p)$, for any a ….. (1)

Again by Wilson's theorem we have,

$-1 \equiv (p-1)!\,(mod\ p)$ …….(2)

Multiplying (1) & (2) we get $-a^p \equiv (p-1)!\,a(mod\ p)$.

Which implies, $a^p \equiv -(p-1)!\,a(mod\ p)$.

Therefore, $p|a^p + (p-1)!\,a$.

b) By Wilson's theorem we have, $-1 \equiv (p-1)!\,(mod\ p)$

This implies, $(p-1)! \equiv -1(mod\ p)$ …….(1)

Also by corollary 5.2 we have $a^p \equiv a(mod\ p)$ ……..(2)

Multiplying (1) & (2) we get $a^p(p-1)! \equiv -a(mod\ p)$

Therefore, $p|(p-1)!\,a^p + a$

Problem 9

If p and q are distinct primes, prove that for any integer a,

$pq|a^{pq} - a^p - a^q + a$.

Solution

By corollary 5.2 we have $x^q \equiv x(mod\ q)$ for any integer x.

Put $x = a^p$ then $(a^p)^q \equiv a^p(mod\ q) \Longrightarrow a^{pq} \equiv a^p(mod\ q)$

This implies, $q|a^{pq} - a^p$ ………… (1)

Also we have, $a^q \equiv a(mod\ q)$, for any integer a.

Which implies $q|a^q - a \dots\dots\dots..(2)$

From (1) & (2) we get,

$q|(a^{pq} - a^p) - (a^q - a) \Longrightarrow\ q|a^{pq} - a^p - a^q + a$

Similarly, we have $p|a^{pq} - a^p - a^q + a$

Therefore, both p and q divides $a^{pq} - a^p - a^q + a$

Hence by corollary 2.7 we have $q|a^{pq} - a^p - a^q + a$

Problem 10

Prove that an odd prime divisors of $n^2 + 1$ are of the form $4k + 1.$

Solution

Let p be an odd prime divisor of $n^2 + 1.$

Therefore, $n^2 + 1 \equiv 0(mod\ p).$

Hence, n is a solution to $x^2 + 1 \equiv 0(mod\ p)$ then we have by theorem 5.5. $p \equiv 1(mod\ 4).$

$\Longrightarrow 4|p - 1$

$\Longrightarrow p - 1 = 4k$ for some $k.$

$\Longrightarrow p = 4k + 1.$

5.3 The Fermat-Kraitchik Factorization Method

Fermat described a technique for factoring large numbers. This represented the first real improvement over the classical method of attempting to find a factor of n by dividing by all primes not exceeding $\sqrt{n}.$

Example 1

Use Fermat's method, let us factor the integer $n = 119143$.

Solution

We know that $345^2 < 119143 < 346^2$

Thus, it suffices to consider values of $k^2 - 119143$ for those k that satisfy the inequality $346 \leq k < \frac{119143+1}{2}$

$$346 \leq k < 59572$$

The calculations begin as follows:

$346^2 - 119143 = 119716 - 119143 = 573$

$347^2 - 119143 = 120409 - 119143 = 1266$

$348^2 - 119143 = 121104 - 119143 = 1961$

$349^2 - 119143 = 121801 - 119143 = 2658$

$350^2 - 119143 = 122500 - 119143 = 3357$

$351^2 - 119143 = 123201 - 119143 = 4058$

$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2$

Hence we get, $119143 = 352^2 - 69^2$

$$= (352 + 69)(362 - 69)$$

$$= 421.283$$

Therefore 421,283 be the two factors of 119143.

Example 2

Use Kraitchik's method, let us factor the integer $n = 12499$.

Solution

The first square just larger than n is $112^2 = 12544$.

So we begin by considering the sequence of numbers $x^2 - n$ for $x = 112, 113, \ldots.$

First we obtaining a set of values $x_1, x_2, \ldots, x_k$ for which the product $(x_i - n) \cdots (x_k - n)$ is a square, say y^2 then $(x_1, x_2, \ldots, x_k)^2 = y^2 \,(mod\, n)$, which might lead to a nontrivial factor of n.

Now, considering the sequence of numbers $x^2 - n$ for $x = 112, 113, \ldots.$

$112^2 - 12499 = 45$

$113^2 - 12499 = 270$

$114^2 - 12499 = 497$

$115^2 - 12499 = 726$

$116^2 - 12499 = 957$

$117^2 - 12499 = 1190$

$118^2 - 12499 = 1425$

$119^2 - 12499 = 1166$

$120^2 - 12499 = 1901$

$121^2 - 12499 = 2142$

or, written as congruences, we get

$112^2 \equiv 3^2.5 \,(mod\ 12499)$ ……………(1)

$113^2 \equiv 2.3^3.5 \,(mod\ 12499)$

$114^2 \equiv 7.71 \,(mod\ 12499)$

$115^2 \equiv 3.2.11^2 \,(mod\ 12499)$

$116^2 \equiv 3.11.29(mod\ 12499)$

$117^2 \ \equiv\ 2.5.7.17\ (mod\ 12499) \dots \dots \dots \dots (2)$

$118^2 \equiv 3.5^2.19\ (mod\ 12499)$

$119^2 \equiv 2.11.53\ (mod\ 12499)$

$120^2 \equiv 1901(mod\ 12499)$

$121^2 \equiv\ 2.3^2.7.17\ (mod\ 12499) \dots \dots \dots \dots \dots (3)$

Since we want the product $(x_i - n)\ \cdots\ (x_k - n)$ is a square. Therefore multiplying $(1), (2)$ and (3) together results in the congruence we get,

$(112.117.121)^2\ \equiv\ (2.32.5.7.17)^2(mod\ 12499)$

That is $1585584^2 \equiv\ 10710^2\ (mod\ 12499)$

Which implies, $1585584\ \equiv\ 10710\ (mod\ 12499)$

Since, we have $gcd(1585584 + 10710, 12499) = 1$ and $gcd(1585584 - 10710, 12499) = 12499$ we get only a trivial divisor of 12499.

Therefore after further calculation we get,

$113^3\ \equiv 2\ \cdot\ 5\ \cdot\ 33\ (mod\ 12499)$

$127^2 \equiv 2.3\ .5.112\ (mod\ 12499)$

Which gives rise to the congruence

$(113.127)^2\ \equiv\ (2.3^2.5.11)^2\ (mod\ 12499)$

Which implies $1852^2 \equiv 990^2\ \ (mod\ 12499)$ and we get

$1852 \equiv 990(mod\ 12499)$

Now, $gcd(1852 - 990, 12499) = gcd(862, 12499) = 431$

Which produces the factorization $12499 = 29.431$.

PROBLEMS 5.3

Problem 1

Use Fermat's method to factor each of the following numbers:

a) 2279

b) 10541

c) 340663

Solution

a) We have $47^2 < 2279 < 48^2$

Thus, it suffices to consider values of $k^2 - 2279$ for those k that satisfy the inequality $48 \leq k < \frac{2279+1}{2}$

$$48 \leq k < 1140$$

The calculations begin as follows:

$48^2 - 2279 = 25 = 5^2$

Therefore $48 - 5 = 43$ and $48 + 5 = 53$ are the factors of 2279

Hence $2279 = 43.53$

b) We have $102^2 < 10541 < 103^2$

Thus, it suffices to consider values of $k^2 - 10541$ for those k that satisfy the inequality $103 \leq k < \frac{10541+1}{2}$

$$103 \leq k < 5271$$

The calculations begin as follows:

$103^2 - 10541 = 68$

$104^2 - 10541 = 275$

$105^2 - 10541 = 484 = 22^2$

Therefore $105 - 22 = 83$ and $105 + 22 = 127$ are the factors of 10541

Hence $10541 = 83.127$

c) We have $583^2 < 340663 < 584^2$

Thus, it suffices to consider values of $k^2 - 340663$ for those k that satisfy the inequality $584 \leq \ k \ < \frac{340663+1}{2}$

$$584 \leq \ k \ < \ 170332$$

The calculations begin as follows:

$584^2 - 340663 = 393$

$585^2 - 340663 = 1562$

$586^2 - 340663 = 2733$

$587^2 - 340663 = 3906$

$588^2 - 340663 = 5081$

$589^2 - 340663 = 6258$

$590^2 - 340663 = 7437$

$591^2 - 340663 = 8618$

$592^2 - 340663 = 9801 = 99^2$

Therefore $592 - 99 = 493$ and $592 + 99 = 691$

Here, 691 is a prime but 493 is not a prime.

Therefore $22^2 < 493 < 23^2$, $(493 + 1)/2 = 247$

Now, consider $23^2 - 493 = 36 = 6^2$

Therefore $23 + 6 = 29$ and $23 - 6 = 17$ are the factors of 493

Hence $17,29,691$ are the factors of 340663

Therefore $340663 = 17.29.691$

Problem 2

Prove that a perfect square must end in one of the following pairs of digits:

$00,01,04,09,16,21,24,25,29,36,41,44,49,56,61,64,69,76,81,84,89,96$

Solution

First we note that $(X + 50)^2 = X^2 + 100X + 2500$, so

$X^2 \equiv (X + 50)^2 (mod\ 100)$.

This means you need to consider the last two digits of

$X = 0,1,2, \dots ,49$ since $0^2 = 50^2$, $1^2 = 51^2, \dots$

But $(X - 50)^2 = X^2 - 100X + 2500$ so

$X^2 = (X - 50)^2 (mod\ 100)$

Therefore, $X^2 \equiv (50 - X)^2 (mod\ 100)$, so for $X = 26,27, \dots ,49$ and $26^2 \equiv 24^2, 27^2 \equiv 23^2, \dots , 49^2 \equiv 1^2$

Therefore, only need to look at digits $X = 0,1,2, \dots ,25$

X	$X^2(mod\ 100)$	X	$X^2(mod\ 100)$	X	$X^2(mod\ 100)$
0	00	11	21	21	41
1	01	12	44	22	84
2	04	13	69	23	29
3	09	14	96	24	76
4	16	15	25	25	25
5	25	16	56		
6	36	17	89		
7	49	18	24		
8	64	19	61		
9	81	20	00		
10	00				

Therefore, the above endings are the ones that were to be proved.

Problem 3

Factor the number $2^{11} - 1$ by Fermat's factorization method **.**

Solution

We have $2^{11} - 1 = 2047$

Thus, we have $45^2 < 2047 < 46^2$

Hence, it suffices to consider values of $k^2 - 2047$ for those k that satisfy the inequality $46 \leq\ k\ <\ (2047 +\ 1)/2\ =\ 1024.$ The calculations begin as follows:

$46^2 - 2047 = 69$

$47^2 - 2047 = 162$

$48^2 - 2047 = 257$

$49^2 - 2047 = 354$

$50^2 - 2047 = 453$

$51^2 - 2047 = 554$

$52^2 - 2047 = 657$

$53^2 - 2047 = 762$

$54^2 - 2047 = 869$

$55^2 - 2047 = 978$

$56^2 - 2047 = 1089 \ = 33^2$

Therefore, $56 - 33 = 23$ and $56 + 33 = 89$ are the factors of $2047.$

Hence, $2^{11} - 1 = 2047 = 23.89$

Problem 4

Factor 13561 with the help of the congruences

$233^2 = 3^2.5\ (mod\ 13561)$ and $1281^2 = 2^4.5\ (mod\ 13561)$

Solution

Given, $233^2 = 3^2.5\ (mod\ 13561)$ and

$1281^2 = 2^4.5\ (mod\ 13561).$

Therefore,

$(233.1281)^2 \equiv (3^2.5.2^4.5) \equiv (2^2.3.5)^2(mod\ 13561)$

Which implies, $298473^2 \equiv 60^2(mod\ 13561)$ and

$298473 - 22.13561 = 131 \not\equiv \pm 60(mod\ 13561)$

Therefore, $gcd(298473 - 60{,}13561) = gcd(298413{,}13561)$

Now, $298413 = 22.13561 + 71$

$13561 = 191.71$

Therefore, $gcd(298413{,}13561) = 71$ which is a prime and also 191 is a prime.

Therefore $13561 = 71.191.$

Problem 5

Use Kraitchik's method to factor the number $20437.$

Solution

Since $\sqrt{20437} = 142.9$

Now, $143^2 - 20437 = 12 = 2^2.3\ \ \ldots\ldots\ldots\ldots..(1)$

$144^2 - 20437 = 219 = 13.23$

$145^2 - 20437 = 588 = 2^2.3.7^2 \ldots\ldots\ldots\ldots(2)$

$146^2 - 20437 = 879 = 3.293$

$147^2 - 20437 = 1172 = 2^2.293$

$148^2 - 20437 = 1967 = 3^2.169$

From (1) and (2) we get,

$(143.145)^2 = (2^2.3.2^2.3.7^2) \equiv (2^2.3.7)^2(mod\ 20437)$

$\Longrightarrow\ (20735)^2 \equiv (84)^2(mod\ 20437)$

$\Longrightarrow\ \ 20735 \equiv 84(mod\ 20437)$

Also, $gcd(20735 - 84{,}20437) = gcd(20651{,}20437)$

Now, $20651 = 20437 + 214$

$20437 = 95.214 + 107$

$214 = 2.107$

Therefore $gcd(20651,20437) = 107$ which is a prime.

Also, $gcd(20735 + 84,20437) = gcd(20819,20437)$

Now, $20819 = 1.20437 + 382$

$20437 = 53.382 + 191$

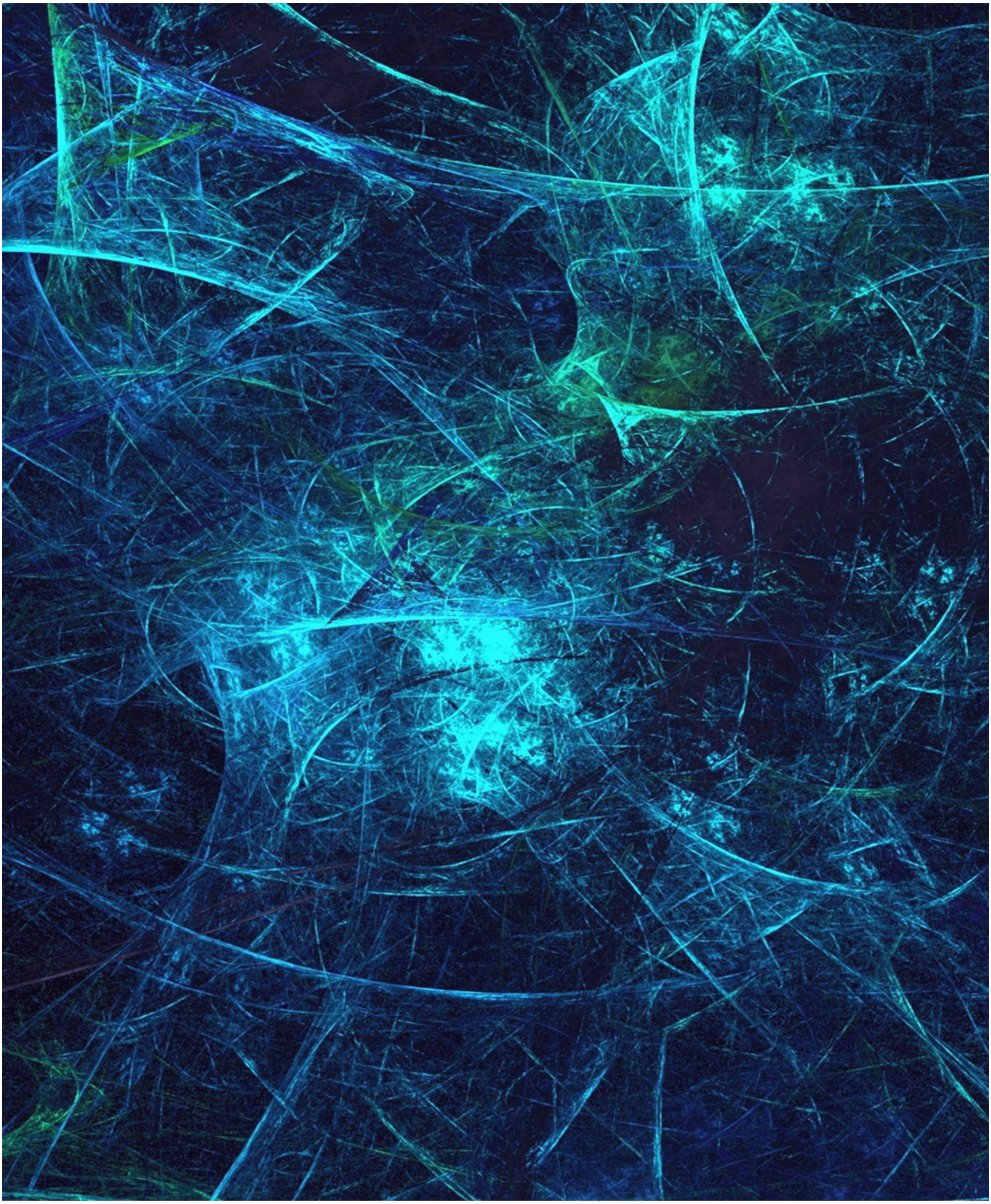
$382 = 2.191$

Therefore $gcd(20819,20437) = 191.$ This is a prime.

Hence, $20437 = 107.191.$

REFERENCES

- Charles Bayd Wren, **Peano's Arioms**
- David M Burton, **Elementry Number Theory.**



Cape Comorin Publisher
Kanyakumari, Tamilnadu, India

ISBN 978-93-88761-28-4
9 789388 761284